VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky

DIPLOMOVÁ PRÁCE

2013 **Bc. David Skowronek**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Analytický software pro automaticky generované eventy

Analytic Software for Automatically Generated Events

2013 **Bc. David Skowronek**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Zadání diplomové práce

Student: **Bc. David Skowronek**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2612T025 Informatika a výpočetní technika

Téma: Analytický software pro automaticky generované eventy
Analytic Software for Automatically Generated Events

Zásady pro vypracování:

Cílem práce je analýza, návrh a implementace analytického software pro eventy generované automatickými monitorovacími nástroji ve společnosti Tieto. Software by měl být schopen poskytnout komplexní pohled na eventy (trendové analýzy), proaktivně vyhledávat a analyzovat abnormality apod., a to z různých pohledů a úrovní (jednotlivý server/zařízení, zákazník, platforma atd.) s primárním cílem redukování celkového počtu eventů a následných incidentů.

1. Požadavky na analýzu eventů (a incidentů) z pohledu ITIL V3.
2. Sběr a analýza požadovaných výstupů na různých úrovních společnosti Tieto.
3. Analýza event management systému z pohledu zpracování eventů a jejich následného ukládání v databázích přístupných analýze.
4. Návrh a implementace analytického software.

Seznam doporučené odborné literatury:

Podle pokynů vedoucího diplomové práce.

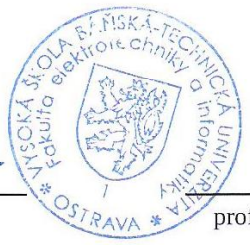
Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Mgr. Stanislav Luzar**

Konzultant diplomové práce: Ing. Jan Kožusznik, Ph.D.

Datum zadání: 18.11.2011

Datum odevzdání: 07.05.2013



doc. Dr. Ing. Eduard Sojka
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně.
Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne 2. května 2013 

Abstrakt

Event Management je jednou z hlavních činností provozu IT, jehož cílem je zpracování značného množství informací, Eventů, zasíláných monitorovacími nástroji. Počty Eventů ve velkých společnostech dosahují desítek milionů měsíčně, v takovémto množství manuální analýza není efektivní. Cílem této diplomové práce je navrhnout a implement analytický software pro společnost Tieto a její implementaci Event Managementu, který by umožnil hromadnou analýzu Eventů a zároveň dokázal reagovat v případě detekovaných abnormalit.

Klíčová slova

ITIL, Event Management, Analytický software

Abstract

Event Management is one the main activities of IT operations aimed at processing of significant amount of information, Events, sent by monitoring tools. Number of Events in large companies reaches tens of millions and manual analysis of such amount of Events is not efficient. The aim of this thesis is to design and implement analytics software for Tieto Corporation and its implementation of the Event Management process, which would allow mass analysis of Events and at the same time being able to react in case of detected abnormalities.

Key words

ITIL, Event Management, Analytic Software

Seznam použitých symbolů a zkratek

AJAX	Asynchronous JavaScript and XML
API	Application Programming Interface
CPU	Central Processing Unit
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	IT Service Management
itSMF	IT Service Management Forum
RAM	Random-Access Memory
SAN	Storage Area Network
SQL	Structured Query Language
URL	Uniform Resource Locator
XML	Extensible Markup Language

OBSAH

1 Úvod

Se stoupajícími nároky v oblasti informačních technologií již společnosti upouštějí od interních IT oddělení a přenechávájí správu svých informačních systémů specializovaným společnostem prostřednictvím tzv. outsourcingu.

Velké nadnárodní outsourcingové společnosti tak mají ve správě desetitisíce serverů a zařízení, která je nutno vzdáleně monitorovat tak, aby byla zajištěna co nejrychlejší reakce v případě problémů. Množství údajů zasílaných monitorovacími systémy je však obrovské a z těchto údajů je potřeba vybrat ty, které vyžadují manuální zpracování, a všechny ostatní uložit pro další zpracování a analýzu.

Tato diplomová práce je zaměřena na vytvoření analytického software pro společnost Tieto, kde v současné době pracuji na pozici Senior Process Manager odpovědný za Event Management, což je proces, který zabezpečuje zpracování údajů zasílaných monitorovacími systémy.

Jelikož každá větší outsourcingová společnost má Event Management nastaven jiným způsobem, který odpovídá jejich aktuálním požadavkům, není v současné době na trhu takový analytický software, které by bylo možno jednoduše upravit pro potřeby společnosti Tieto a její implementace Event Managementu.

V kapitole č. 2 je stručně popsána historie společnosti Tieto, pro kterou je tento analytický software vytvářen.

Vzhledem k tomu, že tato diplomová práce se vztahuje k Event Management procesu, je v kapitole č. 3 stručně popsán ITIL a jeho hlavní charakteristiky. Kapitola č. 4 poté obsahuje popis implementace Event Managementu tak, jak jej ITIL V3 definuje v knize Service Operation, a dále hlavní charakteristiky implementace Event Managementu ve společnosti Tieto.

Kapitola č. 5 je zaměřena na požadavky na analýzu, které jsou popsány v ITIL V3, knize Service Operation, doplněné o specifické požadavky vyplývající z reálné implementance Event Managementu ve společnosti Tieto. Kapitola č. 6 doplňuje požadavky na analýzy o automatické reakce.

Hlavní částí této diplomové práce je kapitola č. 7, kde je popsána praktická implementace analytického softwaru na základě požadavků na analýzy z kapitol č. 5 a č. 6, včetně příkladů výstupů a zhodnocení jejich reálného přínosu na funkčnost Event Management procesu ve společnosti Tieto.

2 O společnosti Tieto

Tieto je největší severoevropský dodavatel IT služeb, poskytující komplexní služby v oblasti IT pro soukromý i veřejný sektor.

2.1 Společnost Tietotehdas Oy

Společnost Tietotehdas Oy vznikla ve finském Espoo v roce 1968. V začátcích zajišťovala vývoj a údržbu IT systémů především pro finskou Union Bank a její zákazníky a také pro lesní průmysl. Portfolio zákazníků v 70. letech rostlo a firma postupně rozšířila své zaměření ze sálových počítačů a softwaru i na osobní počítače a vývoj IT systémů.

V 90. letech zaznamenala rychlý rozvoj díky akvizicím, fúzím a vstupu do strategických aliancí. V roce 1995 změnila své jméno na TT Tieto a v roce 1998 na Tieto. V roce 1996 výrazně pronikla do sektoru telekomunikací akvizicí společnosti Avancer. Od roku 1999, kdy se spojily společnosti Tieto a Enator, nesla jméno TietoEnator.

V průběhu minulého desetiletí se naplno projevila globalizace IT průmyslu a společnost rozšířila své mezinárodní působení. V roce 2004 otevřela první off-shore pobočku v České republice. S příchodem indických hráčů na severoevropský trh zesílila konkurence. Od roku 2007 se firma znovu zaměřuje na severoevropský trh. Zároveň si ale ponechala svůj globální vliv ve vybraných odvětvích, jako jsou telekomunikace.

S podporou horizontálních operací a nárůstem počtu zaměstnanců v off-shore zemích změnila v roce 2009 svou průmyslově orientovanou strukturu na matrixovou strukturu vedení v jednotlivých zemích, průmyslových odvětvích a globálních službách. Do roku 2010 výrazně posílila působení v off-shore zemích. [1]

2.2 Společnost Enator

Skupina Enator vznikla v roce 1995 fúzí s firmou Celsius a.s., kterou koupila v letech 1991 až 1994. Do roku 1994 se o IT operace staraly tři dceřiné společnosti Telub, Enator a Dialog. Fúze dceřiných společností vedla k výrazné restrukturalizaci, dokončené v roce 1997. Na jaře 1996 byla společnost zapsána na stockholmské burze pod názvem Enator. V roce 1998 Enator posílil díky akvizicím. Společnost získala 51 % akcií ve stockholmské konzultační firmě Programmera. Dále převzala dvě malé IT firmy - norský Kvatro Telecom a německý SoftProjekt - a prodala své operace v Enator Telemekanik. V dubnu 1999 společnost Enator koupila dánský NetDesign.

Finská korporace Tieto a švédská společnost Enator se spojily 7. července 1999. Od 26. března 2009 nese společnost název Tieto Corporation. [1]

2.3 Tieto Czech s.r.o.

Do České republiky společnost Tieto vstoupila v roce 2001 a v roce 2004 otevřela své softwarové centrum v Ostravě. S více než 1 900 zaměstnanci je jedním z největších zaměstnavatelů v oblasti poskytování IT služeb v Ćeské republice a největším v rámci Moravskoslezského kraje. Z hlediska počtu kmenových zaměstnanců je česká pobočka společnosti Tieto třetí největší pobočkou Tieto korporace na světě. První dvě místa zaujímají mateřské země Finsko a Švédsko. [1]

3 ITIL

3.1 Co je to ITIL

ITIL je veřejně dostupný rámec, jenž popisuje nejlepší praktiky ve správě služeb IT. Poskytuje rámec pro zvládnutí IT v organizaci, pojednává komplexně o službách a zaměřuje se na neustálé měření a zlepšování kvality dodávaných služeb IT, a to jak z pohledu businessu, tak z pohledu zákazníka. Toto zaměření je hlavní příčinou celosvětového úspěchu ITIL a přispělo k rozšířenému využití a ke klíčovým přínosům, získaným u těch organizací, které aplikovaly tyto techniky a procesy ve svých strukturách.

ITIL ve své současné 3. verzi obsahuje pět ústředních publikací:

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement

Kromě těchto pěti ústředních publikací obsahuje ještě knihu „The Introduction to the ITIL Service Lifecycle“, jež ve stručnosti shrnuje principy uvedené v těchto pěti knihách. Těchto 5 ústředních publikací současně popisuje jednotlivé fáze životního cyklu služby IT. [2]

3.2 Historie vzniku

První verze knihovny ITIL (označovaná jako ITIL V1) spatřila světlo světa koncem 80. let minulého století, kdy britská vládní agentura CCTA, Central Computer and Telecommunications Agency, začala postupně vydávat jednotlivé publikace shrnující nejlepší zkušenosti z oblasti řízení služeb IT (první svazek ITIL V1 vyšel v roce 1989, celá knihovna V1 čítala příjemných 46 svazků).

Klíčovým rysem ITIL již tehdy bylo, že se nejednalo o pravidla vymyšlená úředníky či teoretiky, ale o skutečnou a osvědčenou praxi. Díky tomu, že ITIL obsahoval postupy, které skutečně fungovaly, došlo k jeho rychlému rozšíření mimo britský vládní sektor, pro nějž byl původně určen, a zhruba od přelomu století je ITIL považován za mezinárodně akceptovaný standard pro řízení služeb IT.

Celosvětovému rozšíření ITIL napomohly dvě další významné okolnosti, k nimž došlo na začátku 90. let minulého století:

- **založení sdružení itSMF**, IT Service Management Forum, v roce 1991 ve Velké Británii

  Toto sdružení se zformovalo okolo autorů a recenzentů první verze knihovny s cílem sdílet zkušenosti z oboru ITSM, avšak brzy začaly být zakládány pobočky itSMF i v dalších státech (v ČR až v roce 2006), a to jako neziskové organizace sdružující IT manažery a ITSM specialisty.

- **zavedení mezinárodně akceptovaných certifikací odborné způsobilosti v ITSM**

  Jednotlivé podniky zjistily, že pro řízení informatiky potřebují nejen technicky, ale i manažersky kvalifikované odborníky, a tak začaly pro obsazení klíčových manažerských pozic v IT vyžadovat znalost řízení služeb IT potvrzenou certifikační zkouškou.

Vývoj druhé verze knihovny ITIL (označované jako ITIL V2) započal koncem 90. let ještě pod vedením CCTA. První publikace této druhé verze ITIL, kniha Service Support (některými odborníky považovaná do dnešního dne za nejúspěšnější publikaci v celé historii knihovny vůbec), vyšla v roce 1999.

Důležitým mezníkem v historii ITIL byl zánik agentury CCTA v roce 2000 a převod správy knihovny na nově vzniklou agenturu OGC, jež je vlastníkem pod názvem Cabinet Office ITIL do dnes. OGC pak dokončil vydání druhé verze knihovny, poslední publikace druhé verze vyšla až v roce 2006. V této verzi měla knihovna celkem 10 titulů.

Práce na třetí verzi knihovny ITIL (označované jako ITIL V3) započaly již v dubnu 2004, tzn. dva roky před vydáním poslední publikace druhé verze, a byly završeny 31.5.2007 vydáním pěti ústředních publikací ITIL. Nicméně tím rozvoj třetí verze knihovny zdaleka neskončil – postupně byly a stále jsou vydávány další doplňující a rozšiřující publikace, takže současná podoba knihovny čítá okolo 20 svazků; rovněž je průběžně doplňováno repository dokumentů a databáze znalostí na webovém portálu Best Practice Live. Obsah ITIL tedy není dosud uzavřen.

Pět ústředních publikací ITIL a Výkladový slovník pojmů a zkratek byly v roce 2011 aktualizovány (tato verze je označovaná jako ITIL 2011 Edition); ostatních publikací se tato aktualizace nedotkla.

Přehled historického vývoje ITIL by nebyl úplný bez zmínky o vlivu normy ISO/IEC 20000, která byla vydána 15.12.2005, a to převzetím britské normy BS 15000 do mezinárodního systému ISO. Tato norma je určena k provedení nezávislého certifikačního auditu systému řízení podnikové informatiky založeného na principech ITIL. Přestože první audity byly prováděny již od roku 2003 ještě podle normy BS 15000, do dnešního dne není tato certifikace rozšířena tak, jak se původně očekávalo, a tudíž vliv existence této normy na celosvětovém šíření a používání ITIL není nikterak zásadní. [2]

3.3 Charakteristiky ITIL V3 a hlavní rozdíly oproti ITIL V2

Základní princip ITIL V3 je postaven na řízení životního cyklu služby IT, resp. na řízení hodnoty, kterou informační technologie poskytují svým zákazníkům, tj. odběratelům služeb IT. Ve svých 5 ústředních knihách ITIL V3 popisuje 26 procesů a k nim mnoho desítek dalších aktivit, z nichž mnohé mají charakter celých procesů, a dále 4 komplexní funkce a cca. stovku rolí, které se vztahují jak přímo k jednotlivým procesům, tak souhrnně k celým fázím životního cyklu služby. To však není zdaleka jediný rozdíl oproti V2.

Došlo k obrovskému nárůstu rozsahu prvků „best practice“, které knihovna ve své třetí verzi obsahuje, a přestože nyní již nechybí návody pro řízení služeb IT v celém životním cyklu, tj. nejen v produkčním prostředí, jak tomu bylo ve V2, je pro základní pochopení principů V3 zapotřebí přečíst okolo 1.400 stran pěti ústředních publikací, zatímco pro práci s ITIL V2 stačilo seznámit se s obsahem cca 700 stran knih Service Support a Service Delivery.

Při studiu publikací V3 narazíme na další komplikaci, na kterou jsme nebyli u V2 zvyklí: jednotlivé procesy, aktivity, funkce a role totiž nejsou uzavřeny do jediné fáze životního cyklu služby, ale procházejí jimi napříč, nicméně ústřední knihy V3 jsou psány z pohledu fází životního cyklu služby IT, takže pokud nás zajímá jeden konkrétní proces a jeho aspekty v jednotlivých fázích životního cyklu služby IT, nenalezneme vše přehledně v jedné kapitole jedné knihy, jak tomu bylo u V2, ale je třeba prostudovat téměř všechny kapitoly všech 5 ústředních knih. Tuto nevýhodu do určité míry kompenzují některé z rozšiřujících titulů V3, zejm. čtyři tzv. Capability Handbooks. Toto je daň za to, že ve V3 byl eliminován klíčový nedostatek V2, jímž byl silný akcent na řízení procesů.

Jak bylo řečeno v úvodu této kapitoly: to, co primárně řídíme, nejsou procesy, ale životní cyklus služby IT. Proto by bylo správnější u ITIL V3 hovořit nikoliv o implementaci procesů, rolí, aktivit a funkcí, ale o implementaci prvků „best practice“. Pokud lze procesních výstupů, resp. výsledků, dosáhnout jinak než implementací procesu, je to naprosto v pořádku. Ve V3 je tedy proces, role, funkce či aktivita jen forma aplikace „best practice“, přičemž tato forma není dogmatem.

Při práci s V3 je třeba mít na mysli další důležitou odlišnost od V2: jednotlivé prvky „best practice“ ve V3 již nejsou skládačkou typu „puzzle“, jako ve V2, ale dílky stavebnice typu „lego“, kdy musíme z krabice stavebních kostek vybírat ty, které se nám hodí pro ten typ stavby, kterou vytváříme. Jinými slovy, zdaleka ne všechny prvky „best practice“, které ITIL V3 popisuje, jsou zapotřebí v každém podniku, a zdaleka ne všechny se k sobě hodí.

Příklad: ITIL® V3 obsahuje popis cca stovky rolí, nicméně mnohé z těchto rolí obsahují odpovědnosti, které se navzájem překrývají nebo dokonce vylučují, pokud by byly implementovány v jedné organizaci najednou. S V3 je tedy třeba pracovat tak, že si z krabice stavebních prvků vybereme ty, které jsou pro naši situaci užitečné, a ty použijeme.

Je třeba vycházet z faktu, že ITIL je skutečně sbírkou nejlepší praxe z oboru ITSM, a tudíž vše, co je v něm, uvedeno, je tam uvedeno proto, že se to někde používá a osvědčilo se to. ITIL není univerzálně aplikovatelná metodika, ale rámec, jímž je třeba se nechat inspirovat, a rovněž sbírka prvků „best practice“, z nichž je třeba si vybírat, a jež je nutné přizpůsobovat konkrétní situaci konkrétního prostředí.

Všechny výše uvedené rozdíly oproti V2, zejména komplexita a složitost práce s V3 mají za důsledek, že i téměř 5 let po vydání V3 se mnozí ITSM praktici a IT manažeři v ČR nostalgicky obracejí k ITIL V2. Na druhé straně ITIL V3 je více orientován na byznys potřeby podniku, a proto je o mnoho lépe akceptován z pozic managerů. [2]

4 Event Management

4.1 Definice pojmů

Přestože se tato diplomová práce bude zaobírat zejména Event Management procesem a analýzou Eventů, Event Management proces je úzce spjat i s dalšími procesy, zejména Incident a Problem Managementem. Z těchto důvodů uvedu nejprve definice těchto pojmů tak, jak jsou vedeny v „ITIL® v3 : Slovníček termínů, definic a zkratek“. [3]

Konfigurační položka je jakákoliv komponenta, která by měla být spravována za účelem dodávky služby IT. Informace o všech Konfiguračních položkách jsou zaznamenány v konfiguračním záznamu v Konfigurační databázi a jsou udržovány během jejich životního cyklu Change Management procesem. Konfigurační položky typicky zahrnují hardware, software apod.

Event je změna stavu, která je významná z hlediska řízení Konfigurační položky nebo služby IT. Pojem Event je také používán ve významu výstrahy nebo upozornění pocházející od služby IT, Konfigurační položky nebo monitorovacího nástroje. Event obvykle vyžaduje, aby pracovník provozu IT provedl nějakou činnost a často vede k registraci Incidentu.

Event Management je proces odpovědný za správů Eventů během jejich životního cyklu. Event Management je jednou z hlavních činností provozu IT.

Incident je neplánované přerušení služby IT nebo omezení kvality služby IT. Incidentem je rovněž porucha Konfigurační položky, která dosud neovlivnila službu.

Major Incident je Incident s nejvyšší kategorií dopadu. Následkem Major Incidentu je významné narušení businessu.

Incident Management je proces, který odpovídá za správu životního cyklu všech Incidentů. Hlavním cílem Incident Managementu je co nejrychlejší obnovení služby IT pro uživatele.

Problem je příčina jednoho nebo více Incidentů. Příčina obvykle není známa v čase vytvoření záznamu o Problému a Problem Management je odpovědný za jeho další zkoumání.

Problem Management je proces, který odpovídá za správu všech Problémů po dobu jejich celého životního cyklu. Primárním cílem Problem Managementu je zamezit výskytu Incidentů a minimalizovat dopad Incidentů, kterým nemohlo být zabráněno.

Request for Change (Požadavek na změnu) je formální návrh na provedení změny. Obsahuje detaily navrhované změny a může být zaznamenán papírově nebo elektronicky.

Change Management je proces odpovědný za řízení životního cyklu všech Změn. Primárním cílem Change Managementu je umožnit realizaci prospěšných změn při minimálním narušení služby IT.

Z důvodu jednoznačnosti, a protože analytický software, který je předmětem této diplomové práce, má uživatelské rozhraní v anglickém jazyce, budou v této diplomové práci použítány oficiální anglické výrazy – Event, Incident, Problem atd., nikoliv jejich české překlady.

4.2 Proč implementovat Event Management

Vzhledem ke značnému množství serverů a zařízení, které jsou pod správou outsourcingových firem, není možné reagovat na vzniklé Incidenty teprve ve chvíli, kdy je již zákazník ovlivněn výpadkem či degradací úrovně poskytované IT služby. Je nutné reagovat proaktivně, tj. již ve chvíli, kdy jsou k dispozici první varovné známky blížícího se Incidentu.

Tyto varovné známky pomáhají odhalit monitorovací nástroje, což jsou specializované programy instalované na serverech a zařízeních, které monitorují jejich funkčnost. V případě, že se stav monitorovaného zařízení odchyluje od definovaných parametrů, vytvoří se a odešle Event.

Event Management proces tedy umožnuje proaktivní reakci na blížící se možný Incident, a tím je schopen omezit škody, které by mohly vzniknout v případě plného propuknutí Incidentu.

4.3 Implementace Event Managementu dle ITIL V3

Event Management proces jednotlivé příchozí Eventy třídí do 3 základních kategorií, od kterých se poté odvíjí jejich další zpracovávání:

- **Informational** (informace), kdy je Event vyhodnocen jako informativní, se žádným či velmi malým potenciálním dopadem na chod IT služby. Takovéto Eventy jsou většinou pouze ukládány pro další hromadné zpracování, nebývají řešeny manálně.

- **Warning** (varování), kde se většinou jedná o Eventy vztahující se ke kapacitě IT služeb, jako je docházející místo na disku, velké vytížení CPU, RAM apod. Tyto Eventy ještě neznamenají, že je IT služba nedostupná či degradovaná, koncový uživatel služby nemusí zaznamenat žádné problémy s její dostupností. Jedná se však o včasné varování, které by mohlo přerůst do nedostupnosti služby IT.

- **Exception** (výjimka), kdy už ve velké většině případu je IT služba buď nedostupná či degradována, nebo je její dostupnost v přímém ohrožení.

Takto klasifikované Eventy jsou Event Management procesem dále zpracovány třemi možnými základními způsoby:

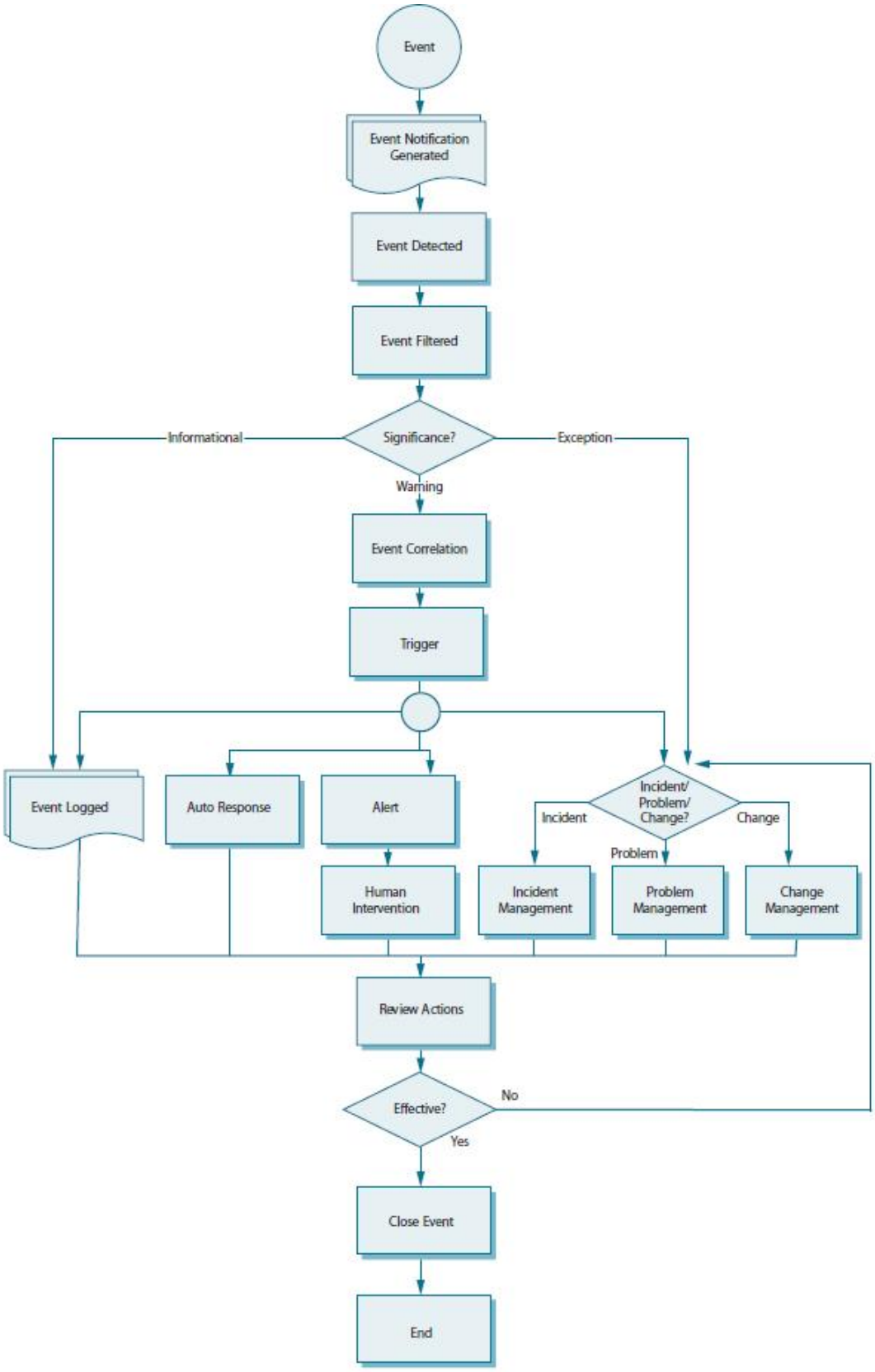
- **Uložení do databáze k následné analýze**. Do databáze jsou zásadně ukládány všechny Eventy nezávisle na jejich klasifikaci, ale pro Eventy kategorie „Informational“ je toto jediná prováděná akce. Nebývají již dále zpracovávány, jsou pouze ukládány pro hromadnou analýzu.

- **Automatická oprava**. Moderní Event Management systémy (software pro zpracování Eventů) umožňují definovat akce, které jsou spouštěny za účelem automatické opravy vzniklých problémů, a to bez nutnosti jejich manuálního řešení. Cílem je zde automatizace řešení vzniklých problémů a tím snížení celkových nákladů. Pokud je automatická oprava úspěšná, Event již není dále zpracováván a informace o úspěšné automatické opravě je uložena do databáze spolu se samotným Eventem.

- **Manuální řešení.** Toto je nejčastější způsob řešení pro Eventy kategorie „Exception“, případně pro Eventy, kde automatická oprava selhala. Dle implementace Event Managementu může být manuální řešení Incidentu inicializováno přímo Eventem, tj. Eventy jsou zpracovávány manuálně, případně je automaticky vytvořen Incident tiket, který je následně řešen.

Kategorizace a způsoby zpracování Eventů popsané výše jsou v zásadě společné pro všechny implementance Event Managementu v hlavních outsourcingových IT společnostech, jelikož vycházejí z popisu Event Managementu v ITIL V2 nebo V3. Zásadní odlišnosti jsou ale v detailech, jak jsou jednotlivé operace v rámci Event Management procesu zřetězeny a implementovány.

Jak jsem již uvedl výše, základní princip Event Management procesu je shodný pro všechny outsourcingové IT společnosti, protože všechny tyto společnosti v dnešní době implementují procesy dle ITIL V2 nebo V3. Event Management proces dle ITIL V3, knihy Service Operation [4], je na následujícím obrázku:



Obrázek č. 1 – Event Management proces dle ITIL V3

4.4 Implementace Event Managementu ve společnosti Tieto

Implementace Event Managementu ve společnosti Tieto vychází z ITIL V3, a proto v zásadě kopíruje schéma Event Management procesu uvedeného v předchozí kapitole. Implementace využívá pro zpracování Eventů sofware od společnosti BMC, a to BMC Event Manager.

Tento software je používán pro zpracování všech Eventů, je však dále rozšířen o množství dalších funkcionalit, které jsou interně vyvinuty a implementovány.

Vzhledem k interní povaze informací o implementaci nelze uvést detaily, proto se omezím pouze na výčet a popis základních charakteristik implementace:

- **Plná automatizace.** Celý Event Management proces, tj. od přijetí Eventu až do rozhodnutí o zvolené akci (např. vytvoření Incident tiketu) ve společnosti Tieto je plně automatizovaný a funguje bez nutnosti manuálních operací. Je využíváno široké škály různých pravidel, od globálních, tj. platících pro všechny příchozí Eventy, až po pravidla platící pouze pro specificky definované Eventy např. z jedné Konfigurační položky. V případě nutnosti pak existují nástroje, a to jak od společnosti BMC tak i interně vyvinuté, kterými je možno v případě problémů s automatizací řešit Eventy manuálně, tj. manuálně provádět jejich klasifikaci a rozhodovat, zda vytvářet Incident tiket apod.

- **Rozšířené filtrování.** V průběhu svého životního cyklu prochází Event v Event Management procesu několika filtry, které rozhodují, zda bude dále Event zpracováván nebo ne. Jsou používány jak inkluzivní defince, tj. metoda „co není povoleno to je zakázáno“, tak exkluzivní, tj. „co není zakázáno to je povoleno“.

- **Kontrola duplicit.** Velmi často jsou generovány duplicitní Eventy, tj. mající ten samý obsah. Z praxe jsem zažil situaci, kdy jeden server byl schopen zaslat 50 000 Eventů během jediné hodiny. Toto množství, pokud by nebyla implementována kontrola duplicit, by bylo schopné totálně zahltit jakýkoliv systém používaný pro správu Incidentů. Proto je v Event Managementu ve společnosti Tieto implementováno několik kontrol duplicit, a to jak již v prvních fázích životního cyklu Eventu, tak i v poslední fázi, jako poslední akce před vytvořením Incident tiketu.

- **Korelace.** Jeden Incident může být zdrojem více Eventů, které přicházejí i z různých Konfiguračních položek. Korelace je proces, během kterého se využívá různých pravidel, jejíž cílem je nalezení těchto souvisejících Eventů a jejich spojení do jednoho jediného. Cílem je, aby ohledně jednoho Incidentu neexistovalo více Incident tiketů, protože by mohla nastat situace, kdy jsou tyto Incident tikety řešeny každý jinou osobou, a jejich řešení by se mohla navzájem ovlivňovat.

- **Detekce Major Incidentů.** Jak je již uvedeno v definicích, Major Incident je Incident s nejvyšší kategorií dopadu na business zákazníka. V těchto situacích je nutno reagovat co nejrychleji, protože každá minuta nedostupnosti IT služby může představovat ve finančním vyjádření ztráty v řádech statisíců i milionů. Proto jsou vyhledávány Eventy, které předznamenávají blížící se Major Incident a nalezená pravidla jsou implementována do Event Managementu tak, že v případě nalezení shody mezi pravidly a generovanými Eventy je možno reagovat na tuto situaci ještě předtím, než Major Incident skutečně vypukne. Tím lze minimálně omezit čas, kdy je IT služba nedostupná, nebo v některých případech vypuknutí Major Incidentu i zabránit.

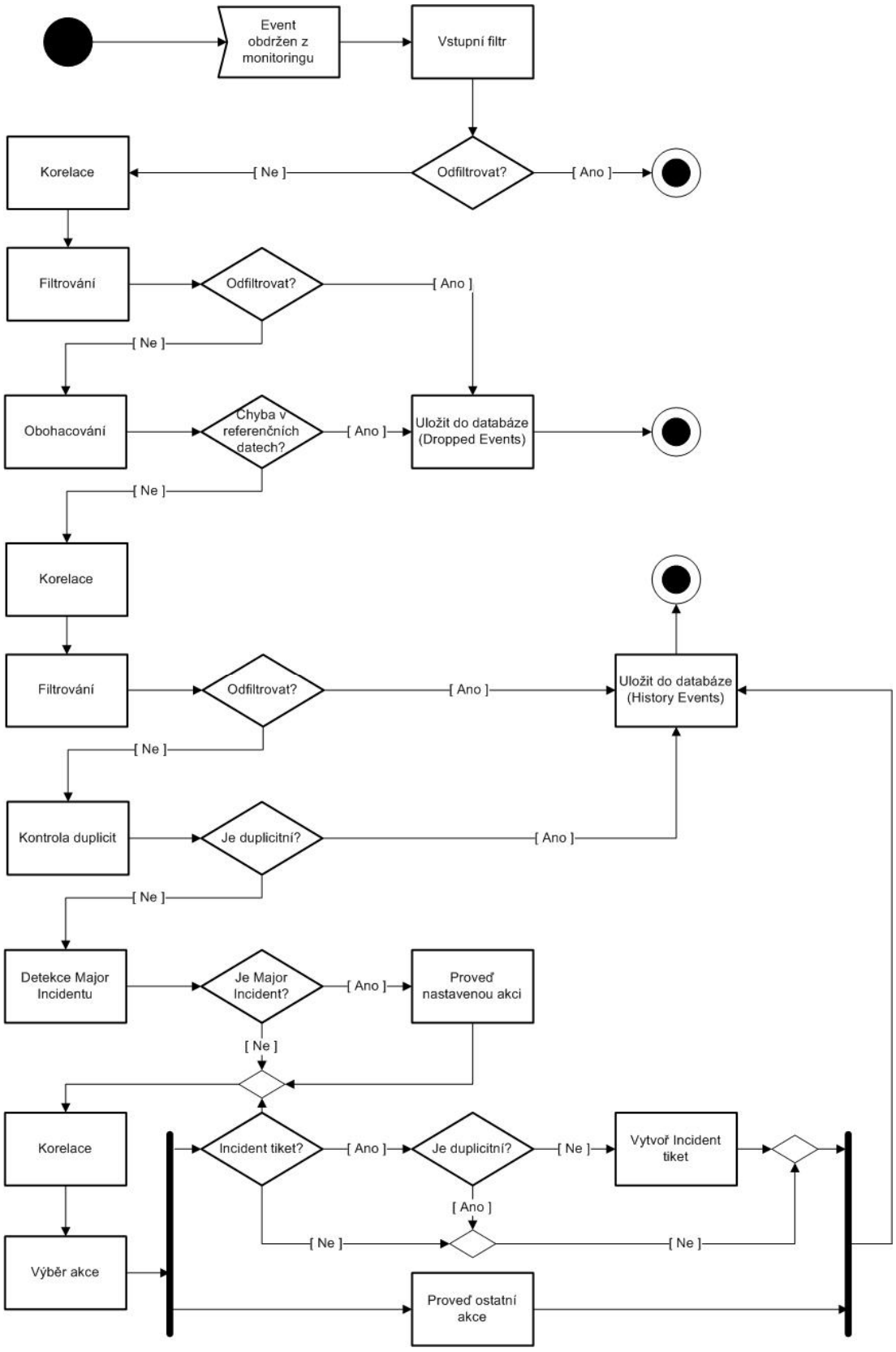
- **Více paralelních výstupů.** Pokud Event projde úspěšně všemi filtry, jako poslední krok se rozhoduje o typu výstupu. V naprosté většině se jedná o Incident tiket, ale pro každý Event je možno definovat i více výstupů najednou, např. zaslání e-mailu, SMS apod.

Obrázek č. 1 s implementací Event Managementu podle ITIL V3 zobrazuje 3 hlavní procesy, které bývají výstupem Eventu:

- Incident Management
- Problem Management
- Change Management

Toto jsou základní procesy, které jsou implementovány v každé velké společnosti zabývající se outsourcingem IT služeb spojených s monitoringem serverů a zařízení. Dle mého odhadu založeného na praktických zkušenostech je Incident Management proces cílem > 99% všech Eventů, Problem a Change Management proces představují jako primární cíl Eventů marginální část.

Následující obrázek č. 2 zachycuje ve značně zjednodušené a zkrácené podobě implementaci Event Managementu ve společnosti Tieto. Jedná se o zjednodušený obrázek zachycující pouze zpracování samotného Eventu, do doby vytvoření Incident tiketu nebo jiné zvolené akce, nikoliv však již následné akce vztahující se k analýze apod., které jsou na obrázku č. 1 zachyceny aktivitou „Review Actions“. Problem a Change tikety nejsou vytvářeny z Eventů automaticky, ale pouze manuálně po jejich analýze.



Obrázek č. 2 – Implementace Event Managementu ve společnosti Tieto

Na první pohled se může zdát, že obrázky č. 1 a 2 jsou naprosto odlišné. Při bližším pohledu je však zřejmé, že obrázek č. 2 pouze obsahuje poněkud detailnější údaje než obrázek č. 1, avšak z obrázku č. 1 plně vychází a sleduje proces zde popsaný.

4.4.1 Rozklad Eventů

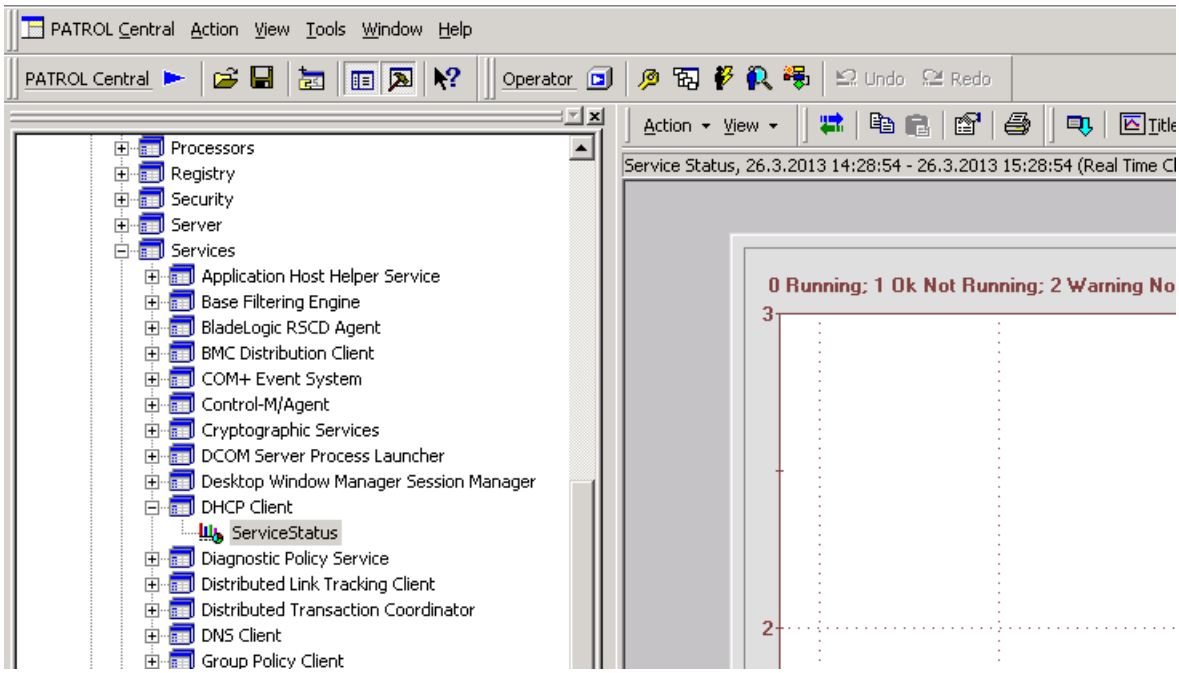
Aby však Event Management byl schopen Eventy vůbec zpracovávat, v první fázi se provede rozložení Eventu na několik parametrů čili atributů. Je jich více než 20, ale pro účely této diplomové práce jsou nejdůležitější následující atributy, se kterými pracuje i analytický software:

- **Configuration Item**, t.j. Konfigurační položka, ze které byl Event vytvořen;
- **Customer**, tj. zákazník, kterému Konfigurační položka patří;
- **Object Class**, tj. klasifikace 1. úrovně, založená na textu Eventu,
- **Parameter**, tj. klasifikace 2. úrovně, založená na textu Eventu,
- **Object**, tj. klasifikace 3. úrovně, založená na textu Eventu.

Toto jsou absolutně nejdůležitější atributy Eventu, které se používají pro nastavování jednotlivých pravidel ve filtrech apod. Kromě nich jsou používány i další atributy, jako např. Severity (Info, Warning, Minor, Major, Critical), Priority (hodnota 1 – 5), atributy vztahující se ke klasifikaci Konfigurační položky (Operation System, Life Cycle apod.), které jsou ale využívány pouze pro specifická nastavení některých funkcí Event Managementu ve společnosti Tieto. Pět atributů uvedených výše však prolíná celým Event Management procesem, jedná se skutečně o základní atributy.

Jelikož atributy Object Class, Parameter a Object budou využívány v analytickém software jako základ pro popis jednotlivých Eventů, pro jejich pochopení je nutné nejdříve vysvětlit způsob, kterým jsou z Eventu samotného získávány.

Pro monitorování stavu serverů a zařízení se ve společnosti Tieto používá široká škála softwaru, nejčastěji se jedná o software společnosti BMC. Na obrázku č. 3 je náhled na BMC Patrol, monitorovací software, který využiji jako první příklad na rozklad Eventů na jednotlivé atributy.



Obrázek č. 3 – BMC Patrol

Na obrázku č. 3 je vidět příklad monitoringu služby „DHCP Client“ operačního systému Windows. Přestože software používaný ve společnosti Tieto pro monitoring serverů a zařízení je různý, uživatelská rozhraní jsou si podobná v tom, že jednotlivé monitorované parametry jsou řazeny ve stromové struktuře. A tato struktura je taky základem pro rozklad Eventů na atributy Object Class, Parameter a Object.

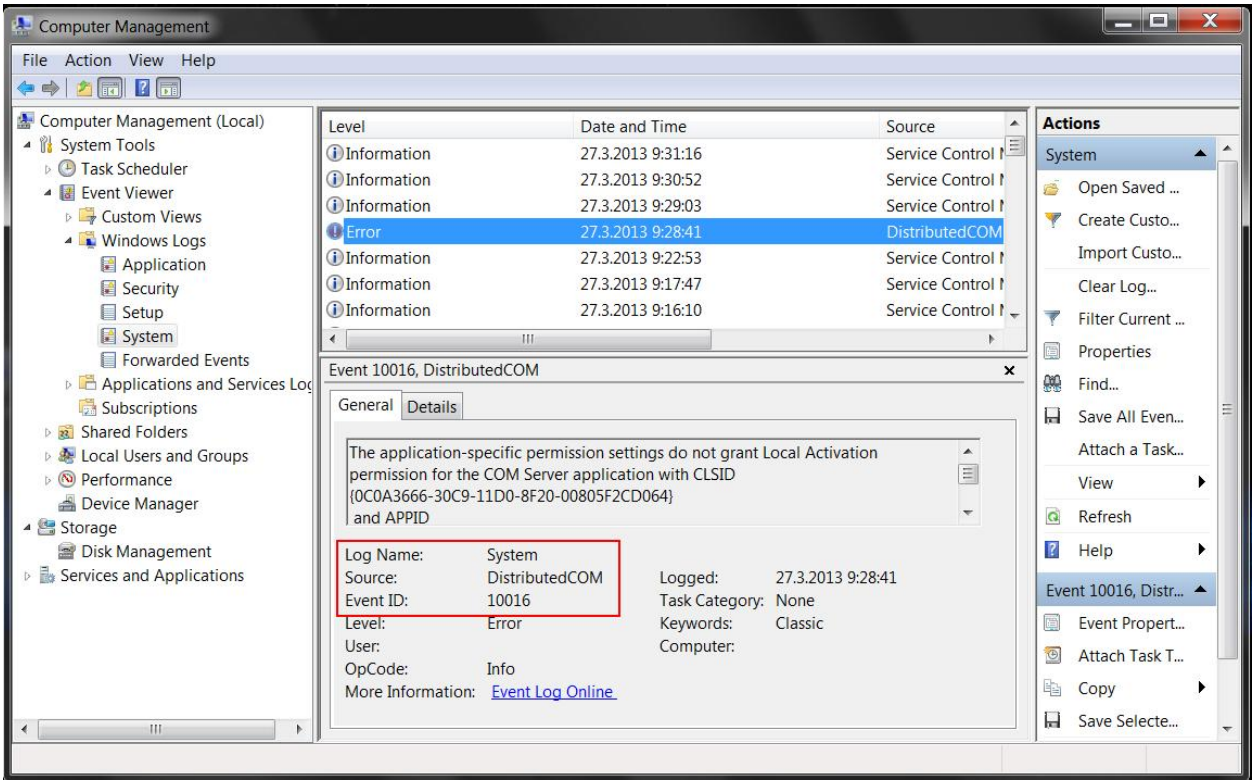
V případě služby „DHCP Client“ na obrázku č. 3 je rozklad následující:

- Object Class = Services
- Parameter = ServiceStatus
- Object = DHCP Client

Atribut „Object Class“ tedy představuje jakousi třídu objektů, atribut „Parameter“ představuje hodnotu, která se monitoruje a atribut „Object“ je potom ta samotná komponenta, která je monitorována.

V případě Eventů, které jsou generovány z logů v operačním systému Windows (viz. obrázek č. 4), je rozklad následující:

- Object Class = název logu (Log Name)
- Parameter = zdroj (Source)
- Object = ID Eventu (Event ID)



Obrázek č. 4 – Windows system log

Podobným způsobem jsou rozkládány i ostatní Eventy, které jsou zasílány různým monitorovacím softwarem, případně jsou přímo generovány pomocí skriptů.

4.4.2 Filtrování Eventů a jejich ukládání do databází přístupných analýze

Jak je na obrázku č. 2 vidět, jsou zde tři možné konce Event Management procesu, kdy je Event buď úplně zahozen bez zápisu do databáze, nebo je zapsán do jedné ze dvou možných databází. Odlišné databáze jsou použity z toho důvodu, že Eventy určené pouze pro analýzu se uchovávají po omezenou dobu a poté jsou vymazány. Eventy, které však projdou úspěšně všemi filtry, tj. jsou důležité a dále zpracovávány (nejčastěji vytvoří Incident tiket), jsou uchovávány v databázi po neomezenou dobu, nejsou vymazávány.

To, zda je Event úplně zahozen bez zápisu do databáze nebo která databáze bude použita pro jeho uložení, je určeno typem filtru či použitou akcí:

- **Odfiltrování vstupním filtrem**

  Vstupní filtr je prvotní rozdělení Eventů na ty, které je potřeba dále zpracovávat a ty, u kterých není zpracování nutné. Každá Konfigurační položka může generovat poměrně velké množství Eventů denně, a při řádově desetitisících Konfiguračních položek (serverů či jiných zařízení v monitoringu) v případě společnosti Tieto to

znamená obrovské množství Eventů, jejich množství se pohybuje řádově ve statisících denně.

Aby se omezila nutnost – z hlediska výkonu softwaru a hardwaru – nákladného zpracování každého Eventu, provádí se již na začátku procesu odfiltrování těch Eventů, u kterých je absolutní jistota, že nemají žádný přínos a není nutné je ani ukládat pro další analýzu. Velmi často se jedná o různé „provozní" Eventy, které slouží ke správnému chodu monitoringu a Event Management infrastruktury, ale nevyžaduje se jich další zpracování.

Tyto Eventy jsou tedy vstupním filtrem odfiltrovány, a nejsou ani ukládány do databází.

- **Odfiltrování inkluzive a exkluzive filtry nebo z důvodů chybějích referenčních dat**

  Jak jsem již uvedl výše v této kapitole, Event Management implementace ve společnosti Tieto využívá pro filtrování Eventů dvou přístupů:

  - inkluzivní metoda

    Tato metoda je založena na přístup „co není povoleno, to je zakázáno". Už z definice této metody je zřejmé, že se jedná o metodu velmi restriktivní a účinnou, ale na druhé straně i potenciálně nebezpečnou. Vzhledem k variabilitě monitorovaných softwarů či hardwarů lze tento přístup použít na velmi specificky omezenou oblast, proto i její využití je velmi omezeno. Na druhou stranu se skutečně velmi osvědčilo a tam, kde je tato metoda použita, je velmi úspěšná.

  - exkluzivní metoda

    Tato metoda je pravým opakem inkluzivní metody a je založena na přístupu „co není zakázáno, je povoleno". Na této úrovni Event Managementu se nacházejí globální pravidla, která platí pro celou platformu (např. operační systém, typ hardwaru či softwaru), nikoliv pravidla pro jednotlivé Konfigurační položky.

Pokud bych použil klasifikaci Eventů popsanou v kapitole 4.3, kde se používají kategorie:

- Informational
- Warning
- Exception

tak se na této úrovni Event Managementu odfiltrovávají Eventy s kategorií Informational a případně Warning, pokud jsou určeny pouze k další analýze a nikoliv pro manuální zpracovávání.

Následně je provedno tzv. obohacování, tj. doplnění dodatečných informací k Eventu z interních databází Event Managementu. Probíhá zde zároveň i kontrola, zda Konfigurační položka je ve správné fázi životního cyklu, kdy je aktivní její monitoring. V případě chybné fáze životního cyklu (tj. chybí referenční data) je Event pouze uložen do databáze, není již dále zpracováván.

Eventy, které jsou odfiltrovány inkluzive a exkluzive filtry nebo důvodů chybějích referenčních dat jsou ukládány do databáze pojmenované **„Dropped Events“**. Tato databáze uchovává Eventy pouze po omezenou dobu, po jejímž uplynutí jsou automaticky mazány. Tyto Eventy slouží pouze pro analýzu, nebývají jednotlivě manuálně zpracovávány. Přestože není nutné zpracovávání jednotlivých Eventů, jejich větší množství již může indikovat potenciální Incident, proto je nutné je analyzovat, sledovat jejich strukturu a množství.

Při zápisu do databáze „Dropped Events“ se k Eventu přiřadí i informace, z jakého důvodu byl do této databáze zapsán, takže je možno rychle dohledat Eventy uložené z důvodů např. chybných referenčních dat apod.

Databáze „Dropped Events“ je sekundární zdroj dat, které budou používány **pro analýzu v analytickém softwaru**.

- **Odfiltrování z důvodu práce na serveru či zařízení nebo z důvodu duplicity**

Event Management implementace ve společnosti Tieto umožňuje několik způsobů, jakým nastavit tzv. blackout, tj. definovat dobu, po kterou probíhá na určité Konfigurační položce práce, která by mohla způsobit generování nechtěných Eventů. Jelikož jsou tyto Eventy nechtěné, jsou přímo způsobené prací na Konfigurační položce, tak mohou být odfiltrovány.

Je možné nastavit dva základní typy blackoutů:

- okamžité uzavření Eventu
- pozdržení Eventu

V případě okamžitého uzavření je tento Event uložen do databáze a není již dále zpracováván. Tato možnost je používána v případě, že po ukončení prací na Konfigurační položce je vždy zkontrolována její funkčnost.

Pozdržení Eventu má oproti okamžitému uzavření výhodu v tom, že v případě přetrvávajících potíží po ukončení prací na Konfigurační položce a odstranění blackoutu jsou ty Eventy, které jsou stále aktivní, dále zpracovány.

Tato funkcionalita je umožněna tím, že monitorovací nástroje umí poslat Event oznamující, že je právě nějaká abnormalita, tj. něco je špatně, ale taky že abnormalita již skončila, tj. vše je v pořádku. Implemenace Event Managementu ve společnosti Tieto tyto dva Eventy spáruje a ony se navzájem vyruší, jsou okamžitě uzavřeny.

Informace o tom, zda byl na Event aplikován blackout, jaký typ blackoutu byl použit a na jakou dobu byl nastaven jsou spolu s Eventem ukládány do databáze.

Následně se provede kontrola na duplicitu vůči ostatním otevřeným Eventům. Kontrola se provádí na základě pěti hlavních atributů uvedených v kapitole 4.1.1 a několika dalších, např. Severity, Priority apod. Pokud je Event označen jako duplicitní, je okamžitě uzavřen a uložen do databáze. Starší Event, který je otevřen, má poté atribut „Repeat Count“ navýšen o hodnotu 1.

Eventy, které jsou odfiltrovány z důvodu práce na serveru či zařízení nebo z důvodu duplicity jsou ukládány do databáze pojmenované **„History Events“**, spolu se všemi ostatními Eventy, které úspěšně prošly všemi filtry.

Databáze „History Events“ je primární zdroj dat, které budou používány **pro analýzu v analytickém softwaru**.

5 Požadavky na analýzu

5.1 Požadavky na analýzu z pohledu ITIL V3

ITIL V3 v knize Service Operation [4] doporučuje sledovat a analyzovat následující hodnoty:

- **Počet Eventů po kategoriích**

  Počet Eventů rozdělených po jednotlivých kategoriích je jedna ze základních analýz, kterou je potřeba implementovat. Kategoriemi se ze nemyslí kategorizace popsána v kapitole 4.3, kde se jednotlivé Eventy kategorizují dle jejich důležitosti na Information, Warning a Exception, ale spíše se zde myslí jednotlivé typy Eventů. Jedná se tedy o typy Eventů, které se dají popsat atributy Object Class, Parameter a Object, jak je uvedeno v kapitole 4.4.1, pojednávající o rozkladu Eventů.

  Zobrazovat výsledky analýz dle kategorií by mělo být možné ve všech analýzách, které budou implementovány, včetně možnosti omezení analýz pouze na Eventy mající určitou kategorii či kategorie.

- **Počet Eventů dle důležitosti**

  Důležitost Eventů je v implementaci Event Managamentu ve společnosti Tieto prováděna atributem Severity, který může nabývat následujících hodnot:

  - Informational
  - Warning
  - Minor
  - Major
  - Critical

  Jedná se o rozšíření klasifikace popsané v kapitole 4.3, protože atribut Severity je jeden z atributů používaných pro výpočet priority Incident tiketu, pokud je vytvořen. Hodnoty doporučované ITIL V3 jsou pouze tři, což není příliš flexibilní, proto byly v implementaci společnosti Tieto tyto hodnoty rozšířeny. Výchozí hodnoty jsou přiřazeny Eventu již monitorovacími nástroji, avšak Event Management má možnost tuto hodnotu jak snížit, tak zvýšit.

Z hlediska důležitosti tato analýza není příliš důležitá, jelikož atribut Severity je pouze jeden z několika atributů používaných pro rozhodování o prioritě vytvářených Incident tiketů. Z tohoto pohledu by bylo lepší mít k dispozici analýzy Eventů dle konečné priority vytvořených Incident tiketů.

Přesto se může ukázat potřebné mít k dispozici analýzy, které mohou ukázat Eventy dle atributu Severity, proto by bylo vhodné ji implementovat.

- **Počet a procentuální vyjádření Eventů, které vyžadovaly manuální řešení a zda bylo manuální řešení provedeno**

  Jelikož je implementace Event Managementu ve společnosti Tieto plně automatizovaná, v případě potřeby manuálního řešení Eventu je vždy vytvořen Incident tiket. Tudíž manuální řešení není na základě Eventů samotných, ale vždy až na základě Incident tiketu.

  Manuální práce je vždy ta nejdražší možná varianta řešení, proto je nutno všechny analýzy zobrazující počty vytvořených Incident tiketů, tj. Eventů vyžadujících manuální řešení, v poměru k počtu Eventů, brát jako ty nejdůležitější.

  V každé analýze, kde je to možné, by mělo být zobraz vždy nejenom počet Eventů, ale zároveň i počet vytvořených Incident tiketů.

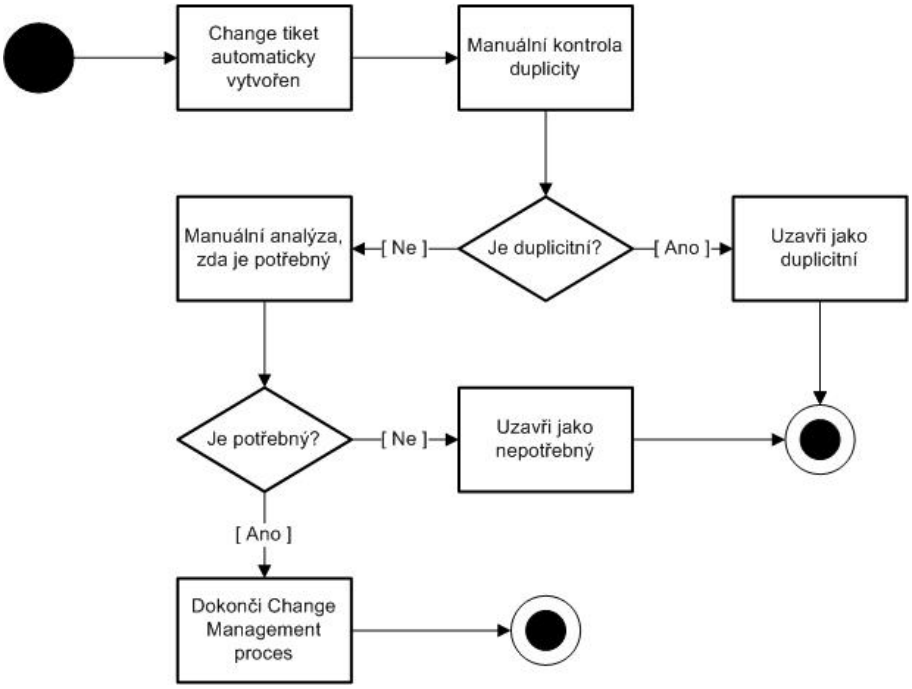
- **Počet a procentuální vyjádření Eventů, které vyústily ve vytvoření Incident nebo Change tiketu**

  Jak je již uvedeno výše, v případě implementace Event Management ve společnosti Tieto potřeba manuálního řešení Eventu = vytvoření Incident tiketu, a důležitost této analýzy již byla popsána.

  Co se týče automatického vytváření Change tiketů přímo z Eventů, toto je v implementaci Event Managementu ve společnosti Tieto možné, software to umožňuje, ale není to používáno v praxi.

  V průběhu návrhu procesu a implementace Event Management ve společnosti Tieto bylo zvažováno, zda implementovat možnost automatického vytváření Problem či Change tiketů přímo z definovaných Eventů, avšak negativa této automatizace převážila nad případnými pozitivy. Proto je tato funkce možná, tj. software ji umožňuje, není však používána.

Pokud by byla tato možnost automatického vytváření Change tiketů implementována, pak by proces jejich následného manuálního zpracování vypadal přibližně následovně:



Obrázek č. 5 – Proces řešení automaticky vytvořeného Change tiketu

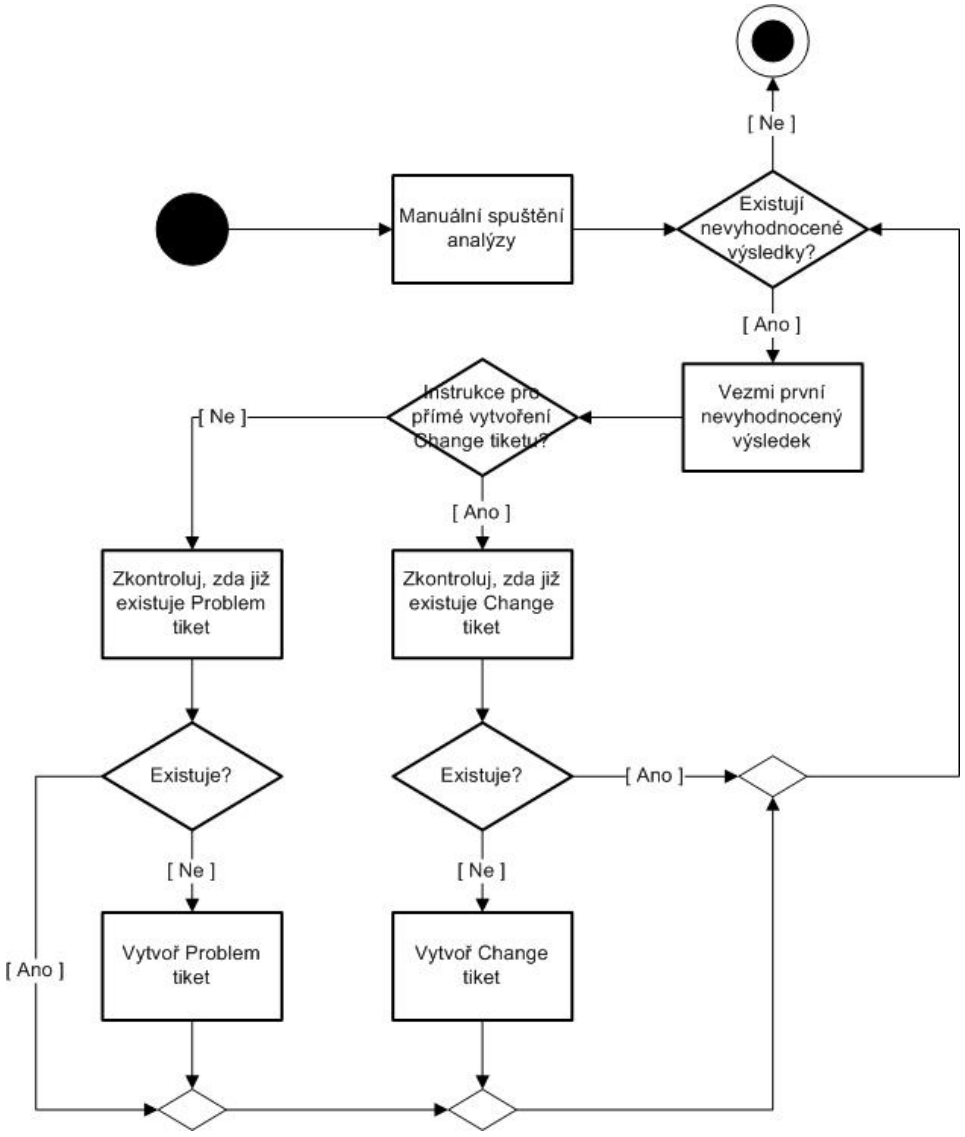
Vzhledem k velkému množství duplicitních Eventů a možnosti manuálního vytvoření Change tiketu, by velké množství automaticky vytvořených Change tiketů bylo duplicitních. Samotná implementace automatické kontroly, zda je již Change tiket vytvořen a definice pravidel, kdy tyto Change tikety vytvářet a kdy ne, případně po jaké době od předchozího automatického vytvoření Change tiketu, by bylo velice náročené.

I přes automatickou kontrolu duplicit vytvářených Change tiketů by bylo nutné každý automaticky vytvořený Change tiket manuálně zkontrolovat na případné duplicity, a zejména provést analýzu, zda v tom kterém aktuálním případě bylo automatické vytvoření Change tiketu skutečně namístě, zda má smysl.

V tomto případě by byla značná potřeba manuální práce, zejména s ohledem na skutečnost, že Change Management proces je proces značně byrokratický. Obdobně by byly řešeny případně automaticky vytvářené Problem tikety.

Z toho důvodu by bylo vhodné použít analýzy Eventů, které jsou nejprve manálně vyhodnocené, a teprve na základě analýz manuálně vytvářet Problem či Change tikety.

Proto je vhodnější v tomto případě postupovat dle následujícího procesu:



Obrázek č. 6 – Manuální vytváření Problem a Change tiketů na základě analýzy

Pokud porovnám proces popsaný na obrázku č. 5, tj. automaticky vytvářet Change tikety (případně Problem tikety), s procesem na obrázku č. 6, kdy se vytvářejí manuálně na základě analýzy, z hlediska efektivity a nákladů vychází proces popsaný na obrázku č. 6 lépe. Na jeho základě jsou vytvářeny smysluplné Problem či Change tikety, kdežto v procesu na obrázku č. 5 dochází k vytváření značného množství duplicitních nebo ne tak smysluplných Problem či Change tiketů.

Pro zlepšení efektivity procesu popsaného na obrázku č. 6 by bylo vhodné mít přímo v analytickém nástroji viditelnou informaci, zda a kolik Problem tiketů je již pro určitou Konfigurační položku otevřeno.

S ohledem na implementaci procesů ve společnosti Tieto je přímé vytváření Change tiketů na základě analýzy Eventů velmi málo využívané, v naprosté většině případů je nejprve zjištěna příčina Eventů prostřednictvím Problem Management procesu, a teprve na základě této analýzy Problému je vytvářen Change tiket. Proto není nutné mít v analytickém nástroji informace o tom, zda a kolik Change tiketů je již pro určitou Konfigurační položku otevřeno.

- **Počet a procentuální vyjádření Eventů, které byly způsobeny existujícími problémy a známými chybami**. Toto může vyústit ve změnu priority práce na těchto problémech nebo známých chybách.

  Tuto informaci by bylo v implementaci Event Managementu společnosti Tieto velmi obtížné získat, jelikož neexistuje přímá vazba mezi Eventy a Problem tikety. Jediná možnost, jak tuto informaci získat, je prostřednictvím Incident tiketů, které jsou propojeny s Problem tikety. Získání těchto údajů by však vyžadovalo vysokou úroveň integrace analytického programu s ITSM softwarem pro správu Incident, Problem a Change tiketů.

  Vzhledem k tomu, že tyto informace mají sloužit pro případné zvýšení priority práce na existujících problémech nebo známých chybách, a přímá implementace této analýzy by byla velice komplikovaná, bylo by možno použít řešení popsané v předcházejícím bodě. Pro každou Konfigurační položku by se zobrazovalo, zda, kolik a jaké Problem tikety jsou právě otevřené. A protože Konfigurační položka je jedním z hlavních atributů Eventu, tato informace bude dostupná v každé analýze.

- **Počet a procentuální vyjádření opakujících se nebo duplicitních Eventů**. Toto může pomoci v úpravě nastavení korelací tak, aby byly eliminovány zbytečné Eventy a také může pomoci při návrhu monitoringu nových služeb.

  Analýza týkajících se opakujících se Eventů je velice důležitá, a to z několika důvodů. Opakující se Eventy:

  - můžou indikovat skryté problémy

    Jakákoliv situace, která se vícekrát opakuje, může indikovat skryté vážnější problémy, i když Eventy samotné můžou mít velice nízkou důležitost. Proto je žádoucí tyto situaci nepodceňovat, jelikož jejich vyřešením lze často předejít Incidentům s vážným dopadem na chod IT služby.

  - zvyšují náklady

    Opakující se Eventy znamenají vyšší nároky na implementaci Event Managementu, jelikož je potřeba mít hardware i software optimalizován na určitý očekáváný počet Eventů. V případě značného množství neřešených opakujících se Eventů se zvyšuje i tlak na upgrade hardwaru a softwaru tak, aby zajistil bezproblémový chod Event Managementu.

Na základě implementace Event Managementu ve společnosti Tieto, zejména na skutečnosti, že je plně automatizována a manuální práce je vyžadována až na základě vytvořených Incident tiketů, bych tuto analýzy rozšířil zejména o analýzu opakujících se automaticky vytvořených Incident tiketů.

Tyto opakující se Eventy, ze kterých se vytvářejí opakující se Incident tikety, se nejvyšší mírou podílejí na zvyšujících se, a zbytečných, nákladech. Velmi často je příčina opakovaných Eventů a Incidentů jednoduše zjistitelná a řešitelná, jelikož často vznikají ze známých příčin jako jsou např. pravidelné restarty služeb v operačním systému Windows, zvýšené využití kapacity disku nebo paměti RAM z důvodu zálohování apod. V těchto případech lze na základě analýzy pouze s minimálními náklady odstranit příčinu těchto opakujících se Eventů a Incidentů, a návratnost nákladů spojených s řešením této situace se často počítá v jednotkách dní.

- **Počet a procentuální vyjádření Eventů, které mohou znamenat kapacitní problémy** (např. jaký vývoj v průběhu posledních 6 měsíců).

- **Počet a procentuální vyjádření Eventů indikujících potenciální problémy s dostupností služby**

- **Počet a procentuální vyjádření jednotlivých typů Eventů po platformách či aplikacích**

Všechny tři body uvedené výše jsou relevantní požadavky na analýzy, ale místo implementací jednotlivých analýz pro každý z těchto bodů zvlášť by bylo lepší implementovat jednu analýzu, kde lze omezit rozsah vstupních dat pouze na specifické Eventy. Omezování vstupních dat by prováděno na základě jednotlivých atributů Eventu, např. Object Class, Parameter a Object. Tyto 3 atributy jsou schopny omezit vstupní data pouze na požadované typy Eventů, např. týkající se pouze kapacity či dostupnosti.

- **Poměr počtu vytvořených Incident tiketů vůči počtu Eventů**

Tato analýza je v implementaci Event Managementu ve společnosti Tieto důležitá z několika důvodů:

  - může odhalit skryté problémy

Vzhledem k tomu, že implementace Event Managementu ve společnosti Tieto umožňuje Eventy pozdržet, tj. Eventy čekají v Event Managementu po určitou dobu, zda dojde k automatické opravě vzniklé situace, mohly by nastat situace, kdy jsou Eventy opakovaně vytvářeny a v rámci jejich pozdržení zavírány. Tato situace je potenciálně nebezpečná, protože všechny Eventy jsou automaticky uzavírány a situace není nijak řešena.

- zlepšování kvality monitoringu serverů a zařízení

Pokud jsou Eventy, které nevytvářejí automatické Incident tikety a zároveň neslouží ani k žádné další analýze, pak mohou být tyto Eventy odstraněny. Odstranění je nejlépe provést co nejblíže jejich zdroji, tj. přímo úpravou nastavení monitorovacího softwaru.

- snižování nákladů

Ideální situací by bylo, pokud by byly generovány pouze ty Eventy, které jsou nějakým způsobem dále zpracovávány, tj. v idálním případě pouze ty, které vytvářejí Incident tikety. Poměr mezi počtem vytvořených Incidentů a Eventů by se měl tedy rovnat či blížit číslu 1.

Dosáhnout takového poměru je však pouze utopií, reálně jej dosáhnout nelze. Pokud by se takovéhoto čísla podařilo dosáhnout, nebylo by nutné mít Event Management, bylo by možné jej přeskočit a vytvářet Incident tikety přímo na základě monitoringu serverů a zařízení.

Tato analýza, pokud by na jejím základě došlo k úpravě nastavení parametrů monitoringu serverů a zařízení, by snížíla náklady na provoz Event Managementu, jelikož by se stávající kapacitou bylo možno zpracovávat Eventy z většího množství serverů a zařízení.

5.2 Požadavky na analýzu ve společnosti Tieto

ITIL V3, kniha Service Operation [4], má poměrně hodně požadavků na analýzu, které nejsou vždy přímo aplikovatelné z důvodu odlišností v implementaci Event Managementu ve společnosti Tieto. Tyto požadavky jsou uvedeny v předchozí kapitole 5.1, avšak z důvodu přehlednosti je shrnu do několika základních požadavků tak, aby byly aplikovatelné na reálnou implementaci Event Managementu ve společnosti Tieto:

- **Počet a typ Eventů a Incident tiketů s možností nastavení časového rozsahu, úrovně detailů zobrazení a možností omezit vstupní data**

V rámci této jedné analýzy se spojuje několik požadavků na analýzu uvedených v předchozí kapitole 5.1. Výstupem této analýzy by mělo být:

- možnost zobrazení dlouhodobého trendu s nastavením typu trendu (lineární, exponenciální, logaritmický apod.);

- možnost zobrazení výsledků pro zvolený časový úsek s úrovní detailů den, hodina, minuta;

- zobrazení počtu Eventů a Incident tiketů pro jednotlivé typy Eventů (dle atributů Object Class, Parameter a Object), dále pro jednotivé zákazníky (atribut Customer) a Konfigurační položky (atribut Configuration Item), případně dle jejich důležitosti (atribut Severity).

Vstupní data by mělo být možno omezovat nastavením filtrů, kde by měla být možnost používat logických spojek, např. „je rovno“, „obsahuje“ apod., včetně jejich negací, nebo výběru ze seznamu v případě pouze několika dostupných hodnot.

Aby bylo možno porovnat zobrazné výsledky a již na první pohled zjistit, zda jsou nějakým způsobem abnormální, bylo by vhodné implementovat zobrazení „normálních“ hodnot. Tyto „normální“ hodnoty by měly představovat středních 60% hodnot, tj. 20% nejnižších a 20% nejvyšších hodnot by bylo odstraněno jako potencionálně abnormálních, nejnižší a nejvyšší hodnota ze zbývajících by poté představovaly dolní a horní hranici „normální“ oblasti hodnot.

Kalkulace by měla být prováděna na dostatenčně dlouhém časovém úseku, minimálně v rozsahu několika měsíců. Dále by měla být prováděna zvlášť pro každý den v týdnu, aby byly zohledněny zejména víkendy.

- **Analýza opakujících se Eventů a Incident tiketů**

Výstupem této analýzy by měly být Eventy a Incident tikety, které se opakují. Tato analýza by měla být spouštěna v pravidelných časových intervalech, s předdefinovanými parametry, zejména pak:

- nastavení časového úseku pro analýzu;
- minimálního počtu Eventů či Incident tiketů, které jsou považovány za opakované;
- nastavení časového úseku, ve kterém musí nastat poslední Event či Incident, aby se zobrazovaly pouze reálné opakující se Eventy a Incidenty, a nikoliv i ty, které již dále nenastávají.

Dále by bylo vhodné implementovat funkcionalitu, která by odhalila vzory v těchto opakujících se Eventech či Incident tiketech. Jednalo by se o vzory typu „tento Incident tiket je vytvářen každý den ve 22:30 +- 5 minut“. Tato funkcionalita by taktéž měla mít volitelně nastavitelné parametry, zejména co se týče +- tolerance pro jednotlivé vzory.

Zobrazení by mělo být dostupné z pohledu:

- Konfigurační položky
- Typu Eventu nebo Incident tiketu

Kromě těchto dvou základních zobrazení by bylo vhodné mít možnost filtrování výsledků tak, aby bylo možné např. zobrazit pouze ty Eventy či Incident tikety, které se týkají pouze kapacity či dostupnosti služby.

- **Poměr počtu vytvořených Incident tiketů vůči počtu Eventů**

  Tato analýza by měla odhalit jak „zbytečné“ Eventy, tj. Eventy ze kterých nejsou vytvářeny Incident tikety, tak i možné problémy spojené s funkcí Event Managementu.

  Možnými problémy se myslí funkce implementace Event Managementu ve společnosti Tieto, kdy určitý Event může být pozdržen a automaticky uzavřen ve chvíli, kdy abnormalita v monitorovaném serveru či zařízení již dále neexistuje. V tomto případě existuje riziko, že k abnormalitě může docházet velice často, avšak Eventy jsou automaticky uzavírány. Tato analýza by měla být schopna odhalit toto chování určitého typu Eventů.

  V analýze by mělo být možno nastavit minimální počet jak Eventů, tak i Incident tiketů, a zároveň definovat časový interval pro analýze. Stejně jako v ostatních analýzách by měla být možnost omezit vstupní data pomocí filtrů.

  Vzhledem k reálné implementaci Event Managementu a ostatních procesů ve společnosti Tieto by tato analýza měla mít výstupy z pohledu:

  - Zákazníka (atribut Customer)
  - Konfigurační položky (atribut Configuration Item)

Tyto tři popsané analýzy pokrývají všechny požadavky na analýzu popsané v ITIL V3, knize Service Operation [4], které jsou uvedené v kapitole 5.1 této diplomové práce. Kromě těchto uvedených analýz je však vhodné mít implementovány ještě další analýzy, které vyplývají z reálné implementace Event Managementu ve společnosti Tieto a z požadavků jak procesu samotného, tak i z individuální požadavků jednotlivých týmů podílejících se na zpracování automaticky vytvářených Incident tiketů.

Na základě těchto požadavků by bylo vhodné implementovat následující analýzy:

- **Analýza dočasných Incidentů**

  Jak je již uvedeno v předcházejících kapitolách, monitorovací nástroje používané ve společnosti Tieto mají schopnost nejenom zaslat Event v situaci, kdy byla detekována abnormalita oproti definovanému stavu, ale zároveň mohou poslat Event v situaci, kdy abnormalita již dále neexistuje.

  Analýza by měla ukázat ty Eventy, ze kterých bych vytvořen Incident tiket a u kterých došlo k automatickému opravení abnormality předtím, než byl Incident vyřešen manuálně.

Takovéto Incident tikety, u kterých došlo k automatické opravě vzniklé abnormality ještě před manuálním vyřešením, jsou neefektivní, bylo by možno uvažovat o pozdržení takovýchto Eventů po určitou dobu, a Incident tiket vytvářet pouze v případě, že po uplynutí definovaného času nedošlo k automatické opravě a tím uzavření Eventu.

Aby bylo možno nastavit správný časový interval pro pozdržení Eventu, analýza by měla ukázat počet minut od vytvoření Eventu a kolik abnormalit bylo automaticky opraveno, i když již byl vytvořen Incident tiket.

Při analýze je ale potřeba vzít v úvahu, že monitorovací nástroje nejsou schopny rozlišit, zda k opravě abnormality došlo automaticky, nebo to je v závislosti na manuální akci. Proto je nutno do analýzy implementovat parametr, který definuje minimální časový interval mezi:

- koncem abnormality detekovaném monitorovacím software a
- manuálním uzavřením Incident tiketu.

Pokud je čas mezi těmto dvěma událostmi větší než definovaný minimální časový interval, pak se jedná o automatickou opravu abnormality. V opačném případě je se jedná o opravu abnormality v návaznosti na manuální akci provedenou na základě Incident tiketu.

- **Analýza záplav Eventů**

Vzhledem ke značnému množství monitorovaných serverů a zařízení ve společnosti Tieto dochází čas od času k záplavě Eventů. Jejich příčina je různá, ale často se jedná o záplavy Eventů způsobené výpadkem některého síťového zařízení, díky kterému jsou tisíce serverů a zařízení odříznuty od monitoringu. V takovém případě je generován z každého takovéhoto zařízení tzv. „connection-lost“ Event, oznamující ztrátu spojení s monitorovaným serverem či zařízením.

Další situací, která může znamenat záplavu Eventů je např. výpadek SAN diskových polí, a jednotlivé servery a zařízení využívající toto SAN diskové pole poté začnou generovat Eventy.

Přestože ne vždy záplava Eventů znamená, že schopnost dodávat IT službu je ovlivněna (může dojít pouze ke ztrátě monitoringu, avšak chod IT služby samotné není ovlivněn, protože segment sítě, ve kterém došlo k výpadku, je používán pouze pro monitoring), jedná se o situaci, která musí být vždy analyzována a které je nutno předcházet. Přesto však může záplava Eventů znamenat nastávající Major Incident, na který je nutno zareagovat co nejdříve, aby se omezily vzniklé škody.

Z toho důvodu by bylo vhodné mít k dispozici analýzu schopnou najít takové Eventy, které předcházejí záplavám. Analýza by se měla spouštět automaticky např. 1x za měsíc, konfigurace by měla zahrnovat:

- nastavení časového úseku pro analýzu;
- dynamickou a statickou metodu pro detekování záplavy, kde dynamická by využívala tzv. „normálního“ průběhu popsaného na začátku této kapitoty, statická metoda pak pevně danou hodnotu;
- procento překročení „normálního“ průběhu (u dynamické metody) nebo počet Eventů (u statické metody);
- nastavení minimální doby trvání záplavy;
- nastavení doby před a po začátku záplavy, během které vyhledávat Eventy, které by mohly záplavu indikovat;
- možnost nastavení minimální úrovně spolehlivosti.

Možnost nastavení doby před a po začátku záplavy, během které se mají vyhledávat Eventy indikující záplavu, je nutné z důvodu specifického chování softwaru pro monitoring, který se ve společnosti Tieto využívá.

Z důvodu snížení zátěže na monitorovaný server či zařízení se ve většině případů neprovádí průběžné monitorování, ale aktuální stav monitorovaného serveru či zařízení je kontrolován v intervalech několika minut, v závislosti na potřebě rychlé reakce na případné problémy.

Z toho důvodu může v některých případech nastat situace, že Event indikující záplavu je odeslán do Event Management systému až po začátku samotné záplavy. Z toho důvodu je nutné nastavit nejenom dobu před zahájením záplavy, ale i po jejím začátku, kde by se měly vyhledávat případné Eventy záplavu indikující.

Analýza by měla zobrazit:

- pro každý nalezený Event indikující záplavu zobrazit v grafické podobě průběh jednotlivých záplav, včetně doby před a po záplavě;
- v záplavě zvýraznit dobu, kdy byl Event indikující záplavu vytvořen a přijat Event Management systémem;
- zobrazit informace o Eventech, které byly během záplavy vytvořeny (jakého jsou typu, od kterých zákazníků či Konfiguračních položek).

6 Automatické reakce

Analytický software, který je tématem této diplomové práce, nemá pouze Eventy analyzovat, ale má být zároveň schopen automaticky reagovat v případě abnormalit. Reakcí se myslí vytvoření Incident tiketu, který upozorňuje na definované abnormality.

Analytický software by měl být schopen automaticky reagovat ve dvou základních případech:

- **počet Eventů v určeném časovém intervalu překročí definované množství**

  Pokud definované množství Eventů určitého typu (může se jednat o jediný typ Eventu nebo o jejich libovolnou kombinaci) překročí definovaný počet, software by měl automaticky vytvořit Incident tiket.

- **sekvence Eventů se stane v určeném časovém intervalu**

  V některých případech je známá sekvence Eventů, která může indikovat potenciální Major Incident. Tuto sekvenci může odhalit zároveň i analýza záplav Eventů posána v předchozí kapitole. Proto je nutno mít implementovánu možnost automatické reakce, tj. vytvoření specifického Incident tiketu v případě, že je tato sekvence detekována.

  Sekvence by měla být definována jako přesná, tj. jednotlivé Eventy musí být ve specifickém pořadí, nebo náhodná, tj. Eventy mohou být v náhodném pořadí. Celá sekvence musí být časově ohraničena.

Analýza a spouštění automatických reakcí by mělo proběhnout vždy po synchronizaci dat s Event Management systémem, tj. poté, co datová pumpa ukončí načítání dat. Pravidla by měla být vyhodnocována třemi základními způsoby:

- zvlášť pro každou Konfigurační položku, tj. pravidlo by se vyhodnocovalo zvlášť pro každou Konfigurační položku, a pro každou Konfigurační položku by se také vytvářel Incident tiket;

- zvlášť pro každého zákazníka, tj. pravidlo by se vyhodnocovalo zvlášť pro každého zákazníka, a pro každého zákazníka by se také vytvářel Incident tiket;

- globálně, tj. vyhodnotit toto pravidlo pro všechny zákazníky a Konfigurační položky najednou, vytvořen by byl pouze jeden Incident tiket.

Vytvářené Incident tikety by měly být vždy spojeny s:

- pevně danou Konfigurační položka;

- náhodně vybranou Konfigurační položkou, kde se vybere jedna z Konfiguračních položek, u kterých byly nalezeny Eventy splňující definované pravidlo.

7 Implementace analytického softwaru

Analytický software, **Event Analytics**, který je cílem této diplomové práce, je její **neveřejnou částí**, a je dostupný pouze z interní sítě společnosti Tieto.

V rámci této kapitoly budou popsány použité technologie, integrace Event Analytics s Event Management systémem ve společnosti Tieto a popsány jednotlivé analýzy a funkce softwaru. V případě použití obrázků softwaru budou zobrazené údaje, jako jsou např. jména zákazníků, Konfiguračních položek apod., anonymizována.

Protože oficiálním jazykem ve společnosti Tieto je angličtina, je i uživatelské rozhraní softwaru Event Analytics v anglickém jazyce.

Při implementaci Event Analytics jsem využil znalostí získaných v předmětu Metody Analýzy Data, ale i z knihy Dobývání znalostí z databází [5].

7.1 Použité technologie a komponenty

Event Analytics využívá pro prezentační vrstu webové rozhraní, která představuje cca 90% zdrojového kódu softwaru, zbylých cca 10% představuje jedenáct .exe a .dll souborů, které jsou využívány např. pro synchronizaci dat nebo náročnější analýzy, které jsou spouštěny v pravidelných intervalech.

Webová část sofwaru se skládá z celkem 75 tříd (Class), 11 modulů (Module) obsahujících definice pro rozšíření (Extension) stávajících tříd a 7 rozhraní (Interface). V tomto počtu nejsou započítávány třídy, které reprezentují jednotlivé webové stránky. Kompilované .exe a .dll soubory obsahují celkem 60 tříd.

Event Analytics využívá dedikovaného serveru s operačním systémem Windows Server 2008 R2 s jedním čtyřjádrovým procesorem, 8 GB paměti RAM a 100 GB pevným diskem vyhrazeným pouze pro Event Analytics a datové soubory.

Event Analytics využívá následujících hlavních technologií:

- **ASP.NET (Visual Basic.NET) 4.0, IIS 7**
- **MS SQL Server 2008 R2**

Celý software, jak webové rozhraní, tak i kompilované .exe a .dll soubory, jsou psány v jazyce Visual Basic.NET ve verzi 4.0.

Dále Event Analytics využívá několika externích komponent, které jsou dle licenčních podmínek zdarma k použití i pro komerční účely. Jedná se o tyto externí komponenty:

- **jQuery** (http://www.jquery.com/), javascriptový framework;
- **jQuery UI** (http://www.jqueryui.com/), nádstavba pro jQuery, sada komponent pro uživatelské rozhraní;
- **Ajax Control Toolkit** (http://ajaxcontroltoolkit.codeplex.com/), sada komponent pro uživatelské rozhraní;
- **PDFsharp & MigraDoc** (http://www.pdfsharp.net/), komponenta pro vytváření PDF souborů;
- **Microsoft Chart Controls for Microsoft .NET Framework 3.5** (http://msdn.microsoft.com/cs-cz/library/dd456632.aspx), komponenta pro vytváření grafů ve webových aplikacích využívajích jazyka .NET;
- **SharpZipLib** (http://www.icsharpcode.net/opensource/sharpziplib/), komponenta pro vytváření .zip archivů;
- **MySql.Data.dll** (http://dev.mysql.com/downloads/connector/net/1.0.html), komponenta pro práci s MySQL databází.

Kromě zde uvedených komponent ještě Event Analytics využívá pro vytváření Incident tiketů nepřímé metody, kdy je využit stávající instalovaný monitorovací software BMC Patrol, jehož prostřednictvím jsou generovány Eventy do Event Management systému, ze kterých jsou následně vytvářeny Incident tikety.

7.2 Agregační funkce pro MS SQL Server

Jelikož Event Analytics pracuje se značným množství dat, která jsou zpracovávána statistickými metodami, agregační funkce dostupné v MS SQL Serveru 2008 R2 nejsou dostačující. Pro rychlejší zpracování dat je součástí Event Analytics i knihovna Analytics.SqlServerFunctions.dll, která je importována do MS SQL Serveru a která obsahuje nové agregační funkce. Jedná se zejména o následující funkce:

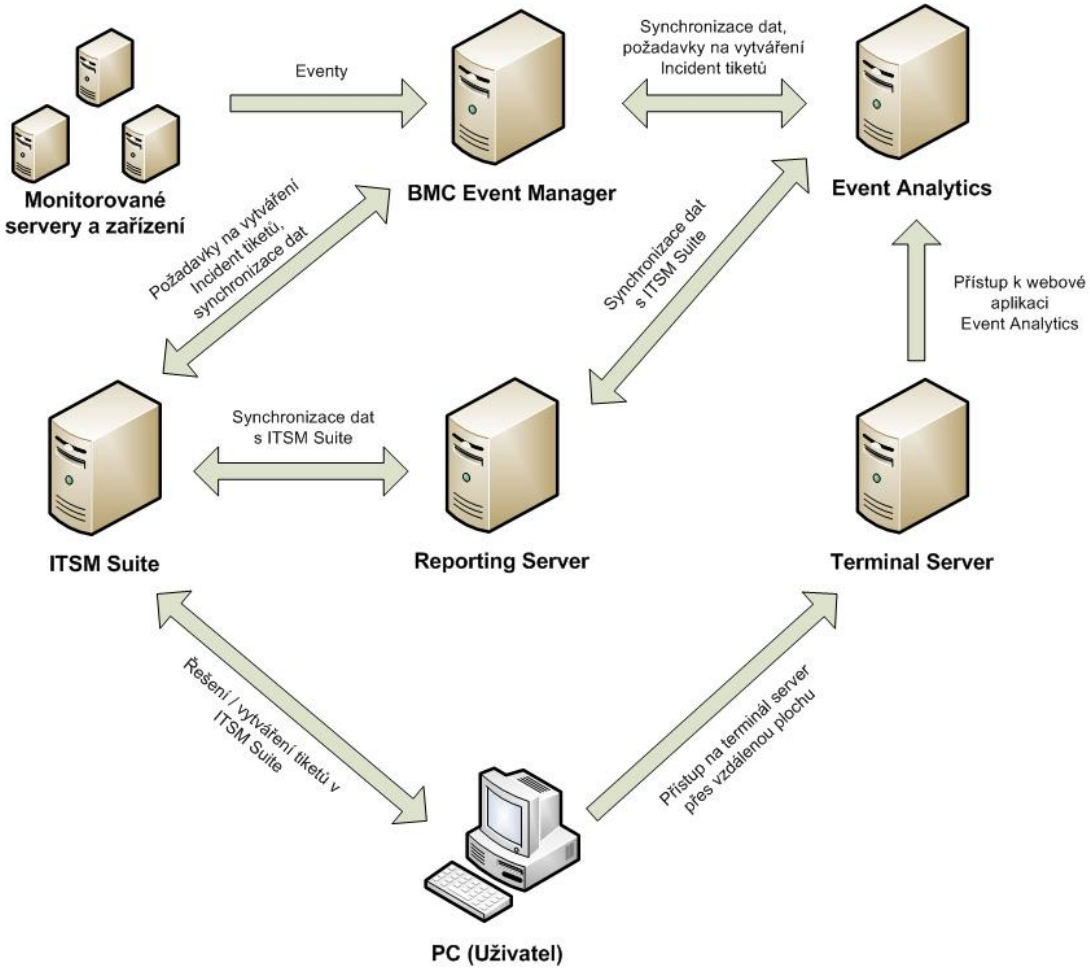
- výpočet průměrné vzdálenosti (časové) mezi jednotlivými Eventy;
- výpočet směrodatné odchylky časové vzdálenosti mezi jednotlivými Eventy;
- výpočet „normálního průběhu“, tj. středních 60% hodnot;
- výpočet korelačního koeficientu.

7.3 Integrace s Event Management systémem

Pro Event Analytics je primárním zdrojem dat databáze Eventů, Dropped Events a History Events, která je součástí Event Management systému. Jelikož však Event Management neobsahuje všechny informace vyžadované pro správnou funkčnost Event Analytics, probíhá také synchronizace přímo s ITSM Suite, ve kterém jsou řešeny jednotlivé Incident, Problem a Change tikety.

Protože Event Analytics neslouží pouze k analýzy Eventů, ale má i možnost automatických reakcí na definované Eventy, je schopen vytvářet Incident tikety. Jejich tvorba neprobíhá přímo, tj. přímou integrací s ITSM Suite, ale je využíváno stávající infrastruktury pro monitoring serverů a zařízení. Server, na kterém je Event Analytics hostován, má instalován monitorovací software BMC Patrol. Event Analytics využívá integraci s BMC Patrol pro vytvoření specifických Eventů, ze kterých jsou následně prostřednictvím Event Management systému vytvářeny Incident tikety.

Následující obrázek č. 7 zachycuje integraci Event Analytics do stávající struktury Event Managementu, včetně způsobu přístupu uživatele k webovému rozhraní Event Analytics.

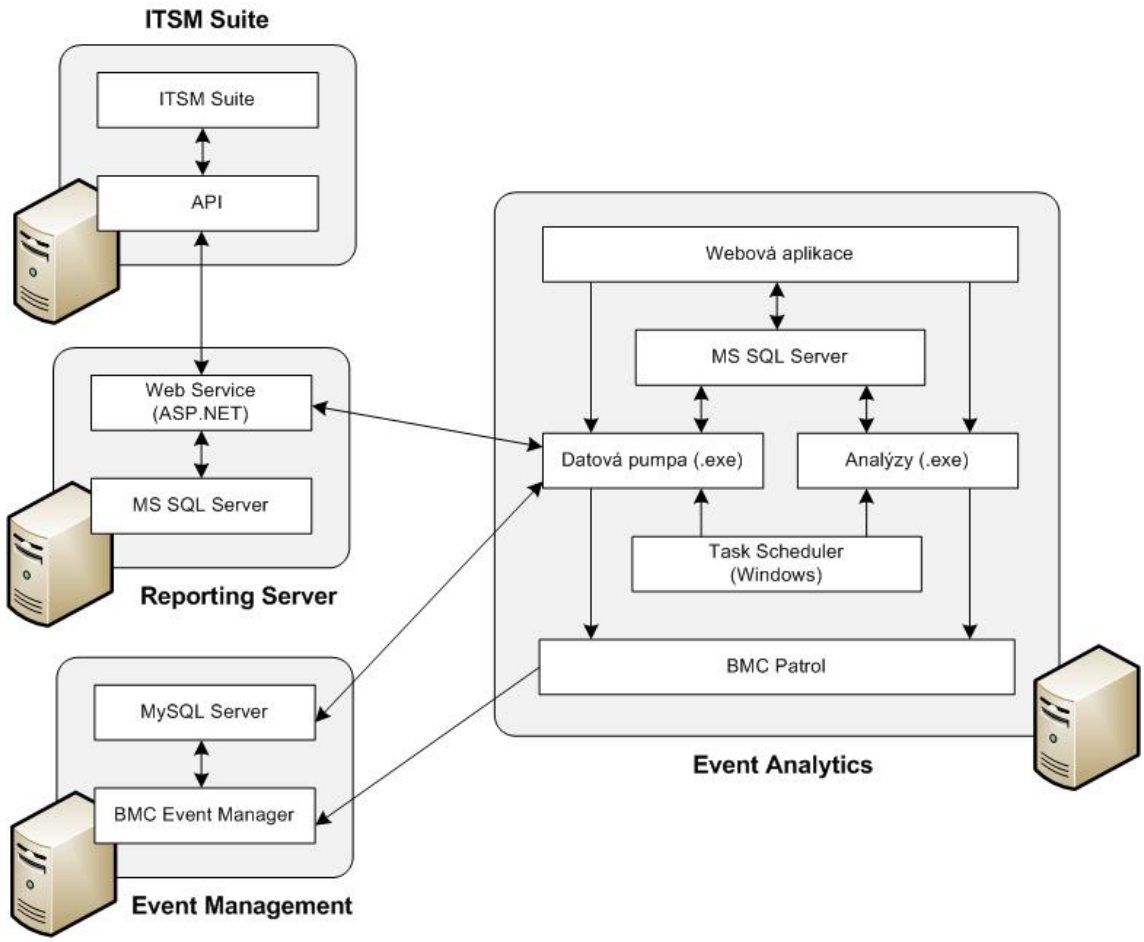


Obrázek č. 7 – Integrace Event Analytics s Event Management systémem

Jak je z obrázku č. 7 patrné a jak je uvedeno na začátku této kapitoly, primárním zdrojem data je Event Management systém, který je na obrázku č. 7 označen jako „BMC Event Manager“.

Sekundárním zdrojem dat je ITSM Suite, tj. software pro správu Incident, Problem a Change tiketů. Protože ITSM Suite je produkční systém a tudíž je nutno omezovat zbytečné čtení dat, synchronizace dat neprobíhá přímo, ale je využíván tzv. Reporting Server, který již obsahuje část dat z ITSM Suite. Reporting Server nejprve vyhledává data ve své interní databázi a teprve v případě, že nejsou dostupná, je dohledá v ITSM Suite.

Pro lepší pochopení integrace Event Analytics s Event Management systémem jsou na následujícím obrázku č. 8 zakresleny datové toky uvnitř Event Analytics, mezi Event Analytics a Event Managementem (BMC Event Manager) a Event Analytics a Reporting Serverem.



Obrázek č. 8 – Integrace Event Analytics s Event Management systémem, datové toky

Synchronizace dat je v Event Analytics prováděna prostřednictvím datové pumpy, jak je zřejmé z obrázku č. 8. Kromě datové pumpy je externí komunikace v Event Analytics prováděna ještě přestřednictví BMC Patrol, tj. instalovaného monitorovacího software, který je využíván v případě potřeby vytvoření Incident tiketu.

7.3.1 Datová pumpa

Datová pumpa je kompilovaný .exe soubor, který je spouštěný v pravidelných intervalech prostřednictví Správce úloh (Task Scheduler) operačního systému Windows. Datová pumpa obsahuje procedury pro synchronizaci dat a jejich transformaci do formátu požadovaného v Event Analytics, analytické procedury, které jsou spouštěny po každé synchronizaci a procedury pro údržbu dat.

Ne všechny procedury jsou spouštěné při každé synchronizaci, interval pro jednotlivé procedury se pohybuje od 1x za 15 minut po 1x za 24 hodin. Datová pumpa může být spouštěna:

- **bez parametrů**

  V případě spouštění bez parametrů jsou jednotlivé procedury, které mají být spuštěny, vybírány automaticky na základě aktuálního dne v týdnu a času. Pro zjednodušení definice ve Správci úloh operačního systému Windows je pravidelné spouštění prováděno bez parametrů.

- **s parametry**

  Spuštění s parametry umožňuje vybrat pouze ty procedury, které je potřeba spustit. Spuštění s parametry je možno jak z příkazové řádky, tak i přímo z webového rozhraní aplikace.

Jak je zakresleno na obrázku č. 7 a v detailu na obrázku č. 8, datová pumpa provádí synchronizaci se dvěma datovými zdroji:

- **Event Management systémem**

  Synchronizace s Event Management systémem je prováděna přímým přístupem do MySQL databáze, kde jsou vyhledány jak nové Eventy, tak i Eventy, u kterých proběhla jejich aktualizace.

  Data, která jsou z Event Management systému načítána, nejsou ve vhodném formátu pro analýzy, jelikož jsou strukturována pro rychlý zápis a změny v Event Management systému. Je potřebná značná transformace dat do formátu použitelného pro analýzy, přičemž některé údaje je potřeba extrahovat i ze strukturovaných textových záznamů (logů).

- **ITSM Suite, prostřednictvím Reporting serveru**

  Jelikož Event Management systém neobsahuje v databázích některé informace důležité pro správnou funkcionalitu Event Analytics, zejména týkající se potřebných údajů o Konfiguračních položkách nebo informace o aktuálně aktivních Problem tiketech apod., je nutné tyto informace získat přímo z ITSM Suite.

Protože ITSM Suite je produkční systém, jsou z důvodu snížení zátěže informace vyhledány nejprve v tzv. Reporting serveru, který většinu potřebných dat obsahuje. V případě, že data nejsou dostupné, tak si je Reporting server vyžádá přímo z ITSM Suite, protože již obsahuje nutné API pro přístup.

Pro integraci Event Analytics (datové pumpy) s Reporting Serverem je využita webová služba (ASP.NET) na straně Reporting Serveru.

7.3.2 Vytváření Incident tiketů

Pro vytváření Incident tiketů není použita přímá integrace s Event Management systémem, ale je použita nepřímá metoda za využití instalovaného monitorovacího software BMC Patrol.

Event Analytics obsahuje třídu, která umožňuje vytvoření specifického Eventu, který je prostřednictvím BMC Patrol zaslán do Event Managementu, který jej zpracuje běžným způsobem a Incident tiket vytvoří. Integrace s BMC Patrol je provedena prostřednictvím jednoduchého skriptu, který je pro BMC Patrol k dispozici:

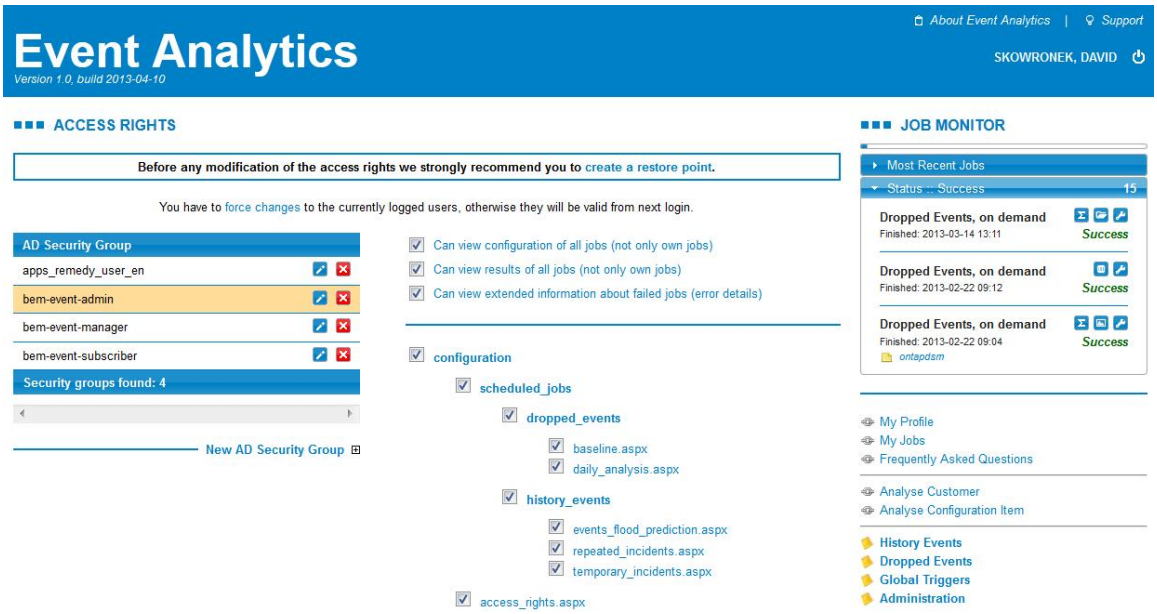
```
user <uživatelské_jméno> <heslo>
connect localhost 3181
execpsl „event_trigger2(<text_eventu_s_parametry>)“
execpsl „event_trigger2(<text_dalšího_eventu_s_parametry>)“
...
exit
```

Vzhledem k jednoduchosti použití byla tatoda metoda upřednostněna před přímou integrací s Event Management systémem v případě potřeby vytváření Incident tiketů.

7.4 Zabezpečení

Přístup k webovému rozhraní Event Analytics je pouze z interní sítě společnosti Tieto, a to pouze přes určené terminálové servery, jak ukazuje obrázek č. 7.

Přístup k webové aplikaci vyžaduje doménový účet, a přístup k jednotlivým analytickým či jiným funkcím je na základě členství uživatele v určených doménových skupinách. Přístup je přiřazován pro jednotlivé webové stránky, tj. .aspx soubory, a editace je přístupná přes webové rozhraní aplikace. Způsob editace přístupových práv je zobrazen na obrázku č. 9.



Obrázek č. 9 – Nastavování přístupových práv

7.5 Nastavení časových zón

Jelikož je společnosti Tieto mezinárodní, s pobočkami ve více zemích s odlišnými časovými zónami, výsledky jednotlivých analýz, ale i nastavování jednotlivých parametrů, jsou vždy dle vybrané **časové zóny uživatele**, kterou si každý uživatel může nastavit ve svém profilu.

K dispozici jsou všechny časové zóny, kde časový posun je o celou hodinu. Časové zóny, kde je časový posun např. + 05:30, nejsou v nastavení k dispozici. Odstranění těchto časových zón je z důvodu nutnosti rychlého zpracování výsledků.

Výsledky jsou často seskupovány po minutách či hodinách (např. počet Eventů vytvořen během určité hodiny) a z toho důvodu jsou v databázi již uloženy i upravené časové hodnoty, kdy např. čas vytvoření Eventu 12.4.2013 15:23:58 je uložen zároveň jako 12.4.2013 15:23:00 (pro seskupování po minutách) a 12.4.2013 15:00:00 (pro seskupování po hodinách).

Díky odstranění časových zón, kde posun času není o celou hodinu, lze výsledky rychle zpracovat za použití GROUP BY funkce a poté posunout časovou hodnotu dle nastavení uživatele.

V případě použití časových zón, kde posun je i o část hodiny (např. + 05:30), není možné rychlé zpracování výsledků, jelikož by mohla nastat následující situace:

	UTC+00:00	*UTC+02:00*	*UTC+05:30*
Čas vytvoření Eventu	15:45:25	17:45:25	21:15:25
Čas pro seskupování po minutách	15:45:00	17:45:00	21:15:00
Čas pro seskupování po hodinách	15:00:00	17:00:00	**20:30:00**

Jak je vidět z tabulky časů, v případě posunutí časové hodnoty pro seskupování po hodinách o + 05:30 již nebude červeně označená hodnota správná. Správná hodnota by byla 21:00:00.

Pokud by byly takovéto časové zóny povoleny, zpracování výsledků analýz by trvalo mnohem déle, protože GROUP BY funkce by nemohla být použita na časové hodnoty po hodinách, ale pouze po jednotlivých minutách, které by musely být následně časově posunuty a teprve poté zpracovány do finálních časových hodnot.

V případě zpracování výsledků jednoho dne by místo 24 záznamů (1 záznam = 1 hodina) bylo nutno zpracovat 1440 záznamů (1 záznam = 1 minuta), které by musely být časově posunuty a poté seskupeny po hodinách.

7.6 Spouštění analytických funkcí

Jednotlivé analytické funkce, které jsou v Event Analytics k dispozici, využívají několika přístupů ke zpracování, které se liší podle jejich náročnosti a času potřebného ke zobrazení výsledku:

- **pravidelně spouštěné analytické úlohy**

  U některých implementovaných analýz, např. pro vyhledávání opakujících se Eventů a Incidentů, je předpoklad jejich velmi častého využívání a zároveň je zde poměrně velká časová náročnost na výpočty.

  V případě kombinace časové náročnosti a častého využívání jsou takového analytické funkce implementovány jako kompilované .exe soubory a spouštěny automaticky v definovaných časových intervalech prostřednictvím Správce úloh operačního systému Windows. Takového analýzy jsou vypočítány a jejich výsledky jsou uloženy v databázi s možností jejich okamžitého zobrazení.

- **úlohy „na vyžádání“ s odloženým zobrazením výsledků**

  Databáze obsahují Eventy, které byly odfiltrovány a jsou pouze ukládány pro další zpracování, tj. databáze „Dropped Events“, obsahuje desítky milionů Eventů. A to přestože jsou uchovávány pouze po omezenou dobu.

Přestože databáze obsahuje pro tyto záznamy velké množství indexů, zpracování některých analytických úloh vyžaduje několik minut. Aby uživatel nemusel po tuto dobu čekat bez možnosti práce s Event Analytics, jsou tyto náročné analytické úlohy spouštěny jako externí úlohy, během kterých nehrozí uplynutí časového limitu pro zobrazení webové stránky a uživatel může bez omezení pracovat s Event Analytics.

Analytické úlohy jsou spouštěny prostřednictvím kompilovaných .exe souborů, které mají jako vstupní parameter ID úlohy, která je uložena v databázi a kde je XML soubor s její konfigurací. Během zpracování úlohy je průběžně aktualizován její stav, tj. kolik % je již hotovo, což uživatel může sledovat v Monitoru úloh (Job Monitor). Monitor úloh je aktualizován v pravidelných intervalech použitím jQuery AJAX technologie, takže uživatel má přehled o aktuálním stavu zpracovávané úlohy, jak je vidět na obrázku č. 10.

Obrázek č. 10 – Monitor úloh s právě probíhající úlohou

V rámci jedné analytické úlohy je možno zvolit více různých výstupů, které jsou na obrázku č. 10 reprezentovány jednotlivými ikonami:

- graf + sumář Eventů po atributech;
- sumář Eventů dle vybraného atributu;
- kompletní výpis Eventů (je omezeno maximálním počtem);
- export Eventů do .csv souboru (je omezeno maximálním počtem).

- **úlohy s okamžitým zobrazením výsledků**

V případě, že zpracování a zobrazení výsledků úlohy trvá do cca 30 sekund, analýza je spouštěna přímo webovou aplikací a webová aplikace čeká na zobrazení výsledků. Pro vylepšení výkonu jsou výsledky těchto úloh dočasně – do doby další synchronizace dat – ukládány do databáze za pomocí binární serializace. Webová aplikace se vždy nejprve pokouší najít a použít tyto dočasné výsledky, a teprve v případě neúspěchu spouští novou analýzu.

- **kombinované úlohy**

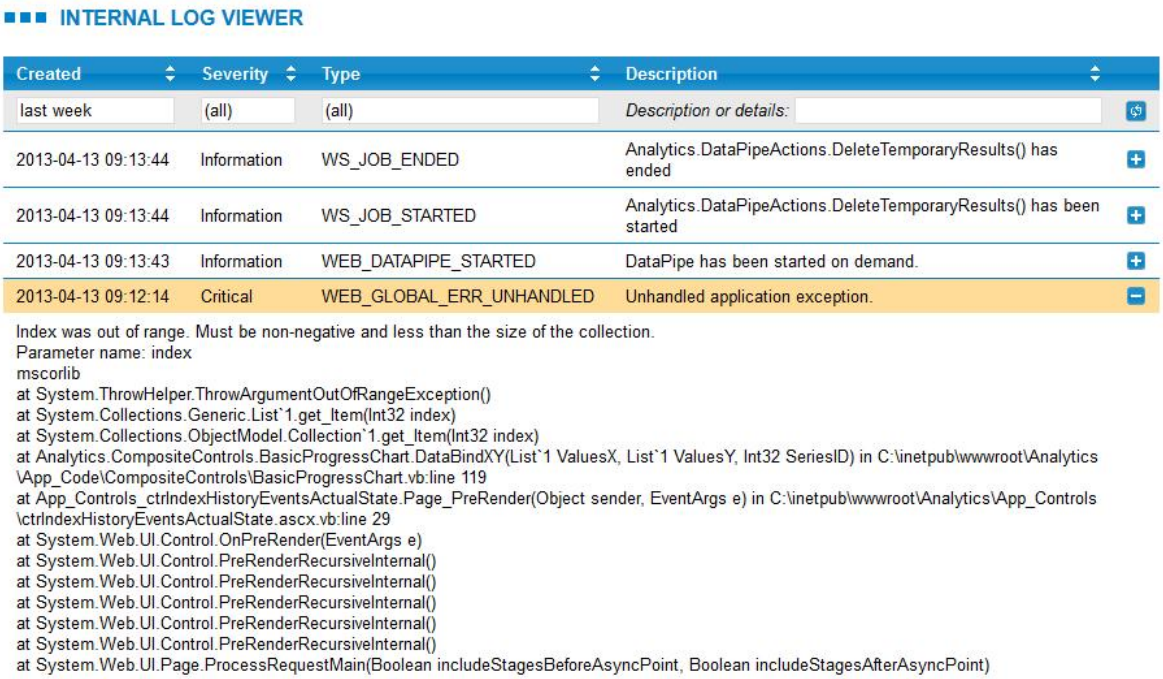
  U některých analýz se používá kombinovaného přístupu, tj. analytická úloha je pravidělně spouštěna za pomocí Správce úloh operačního systému Windows a v rámci této analýzy jsou provedeny základní výpočty a vyhodnocení.

  Zobrazení výsledků analytické úlohy může např. vyžadovat grafickou interpretaci, a předpočítat údaje pro všechny možné výsledky analytické úlohy by bylo značně časově náročné. V takových případech, kdy navíc výsledky nejsou pravidelně vyžadovány více uživateli, jsou předpočítány pouze základní údaje, které uživateli poskytnou dostatečné informace pro posouzení, zda je nutno se výsledkem analýzy zabývat či ne. Pokud si uživatel zobrazí detailnější informace o výsledku analýzy, tyto detaily již nejsou předpočítány, ale jsou dopočítány a zobrazeny přímo webovou aplikací.

7.7 Logování chyb

Event Analytics obsahuje interní log, ve kterém jsou jak záznamy o chybách v aplikaci, tak i záznamy např. o spouštěných analytických úlohách či změnách v konfiguraci.

Případné kritické neřešené chyby v aplikaci jsou zachytávány v modulu Global.asax, a automaticky zapisovány do logu, všechny chyby obsahují i detailní informace (StackTrace).



Obrázek č. 11 – Interní log

7.8 Filtrování výsledků

V Event Analytics jsou implementovány 2 typy filtrování výsledků analýzy či omezování vstupních data pro analytické úlohy:

- **jednoduché filtrování tabulkových výpisů**

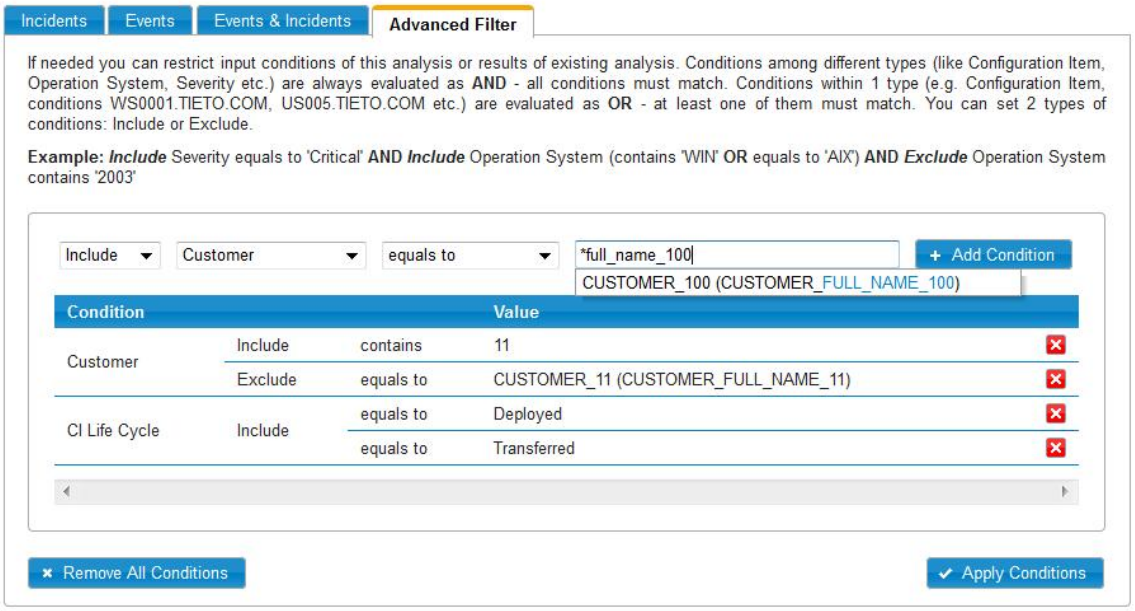
  V případě zobrazení výsledků ať již analýzy, nebo např. záznamů v logu, je možno tabulkový výpis záznamů filtrovat pomocí filtru umístěného v záhlaví tabulky. Jedná se rychlé filtrování, kde nelze nastavovat komplexní podmínky. Příklad tohoto filtru je viditelný na obrázku č. 11.

- **rozšířené filtrování**

  V případě potřeby je možno filtrovat výsledky analýzy nebo omezit vstupní data analýzy za pomocí rozšířeného filtrování, kde lze nastavovat kombinace podmínek.

  Rozšířený filtr je implementován jako samostatná komponta, kterou lze umístit na webovou stránku, a nastavit atributy, které lze ve filtru použít. Konfigurace aktuálního filtru je vždy ukládána do databáze, komponenta rozšířeného filtru si automaticky přidává do URL adresy unikátní ID filtru, jehož konfiguraci si poté načte z databáze.

  Pro jednoduchou aplikaci rozšířeného filtru je připraveno rozšíření (Extension) třídy System.Data.SqlClient.SqlCommand, jehož použitím je SQL dotaz upraven dle aktuálního nastavení rozšířeného filtru, jehož ID se nachází v adrese URL.

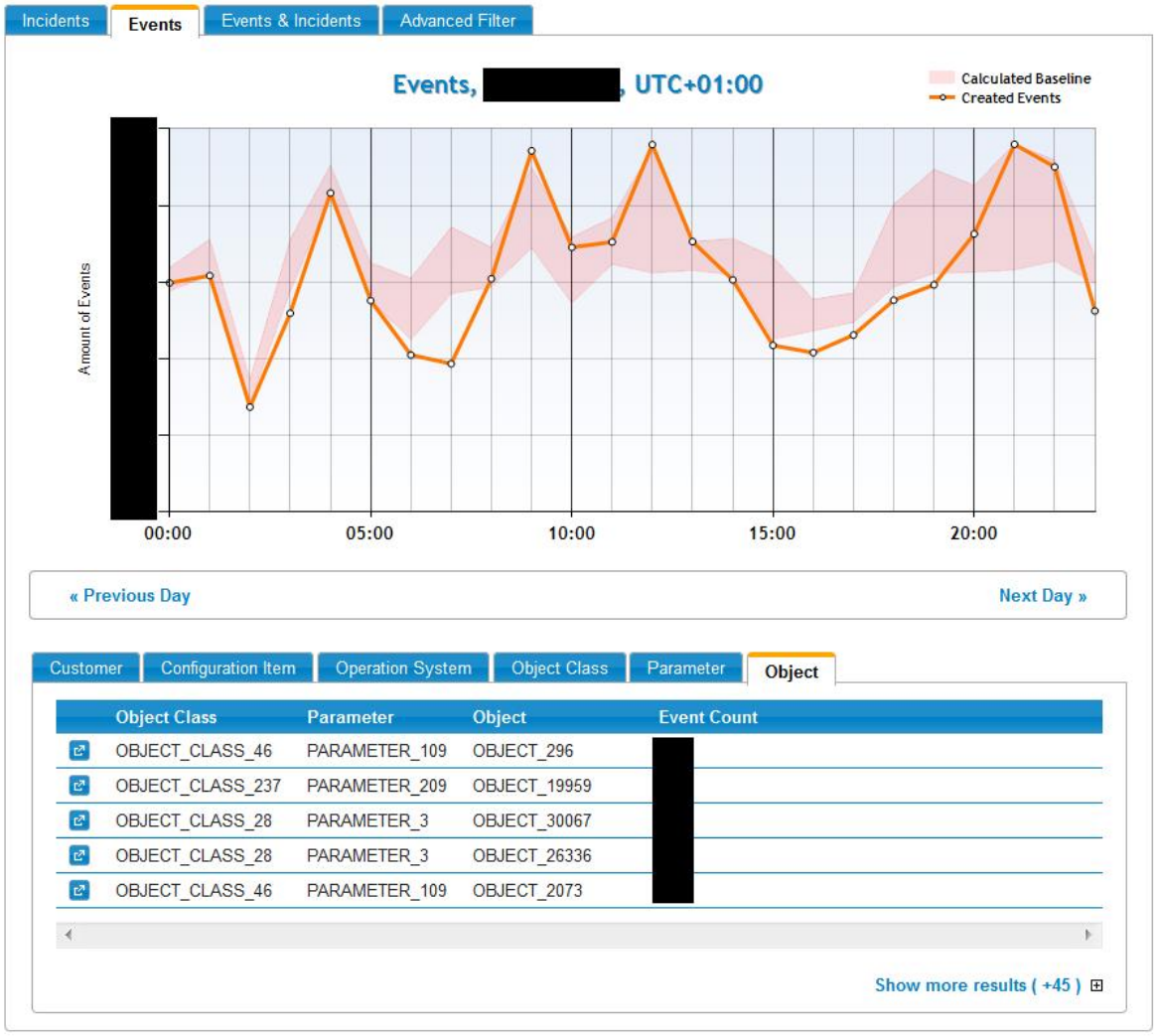


Obrázek č. 12 – Rozšířený filtr

7.9 Implementované analytické funkce

7.9.1 Vytváření Eventů a Incident tiketů v čase

Tato analýza je velmi často využívána, jelikož umožňuje na první pohled poznat, zda se množství Eventů či Incident tiketů odchyluje od normálního očekáváného průběhu. Díky zobrazeným detailům lze velice rychle zjistit rozsah abnormality, tj. zda se jedná o globální abnormalitu nebo o lokální, zahrnující jednoho zákazníka či Konfigurační položku.



Obrázek č. 13 – Vytváření Eventů v čase (s anonymizovanými údaji)

Jak je z obrázku č. 13 patrné, opravdu lze na jeden pohled zjistit, zda dochází v průběhu vytváření Eventů k abnormalitám či ne. Oblast značená jako „Calculated Baseline“ představuje „normální“ průběh, tj. středních 60% hodnot.

V případě databáze „History Events“ je k dispozici Rozšířený filtr, který lze použít k omezení vstupních dat. Kromě Rozšířeného filtru je možno pro filtrování ještě použít ikonu , která přidá vybrané podmínky do Rozšířeného filtru.

Jelikož však databáze “Dropped Events” obsahuje cca 100x více záznamů než databáze “History Events”, v případě použití Rozšířeného filtru by byl, i přes značné množství indexů, čas potřebný ke zobrazení výsledků neakceptovatelný. Proto nelze v případě databáze “Dropped Events” používat rozšířený filtr, ale pouze filtrování pomocí ikony  . Lze však kombinovat podmínky z různých atributů (Customer, Configuration Item atd.).

V případě potřeby lze pro databázi “Dropped Events” využít analýzy na vyžádání, kde lze použít Rozšířený filtr, a která je spouštěna prostřednictví .exe souborů na pozadí. Zobrazený výsledek (výstup) je naprosto stejný, jako na obrázku č. 13.

Pro zobrazení vytváření Eventů a Incident tiketů v čase lze použít následující analýzy, mezi kterými lze přecházet kliknutím na hodnotu v grafu:

- **dlouhodobý trend**

  Dlouhodobý trend je k dispozici jak pro databázi „History Events“ tak i „Dropped Events“, i když Eventy v databázi „Dropped Events“ jsou ukládány pouze po omezenou dobu. V případě databáze „Dropped Events“ jsou trendové hodnoty předpočítány a uloženy do databáze.

  Tato analýza nedovoluje zobrazit detaily, které jsou na obrázku č. 13 viditelné pod grafem samotným. Důvodem je značná časová náročnost v případech, kde uživatel potřebuje zobrazit trend např. za celý rok.

  U dlouhodobého trendu je možnost zobrazit i trendovou linii, k dispozici jsou následující možnosti:

  - lineární;
  - polynomiální;
  - exponenciální;
  - logaritmický.

- **vybrané dny**

  Tato analýza, stejně jako obě následující (jeden vybraný den a vybraná hodina) jsou dostupné pouze v případě, že jsou Eventy v databázi. V případě databáze „Dropped Events“ jsou tedy dostupné pouze po omezenou dobu.

  V rámci této analýzy lze zobrazit v aktuální konfiguraci max. 14 dní, v grafu jsou výsledky (počty Eventů) seskupeny po jednotlivých dnech.

- **jeden vybraný den**

  Zobrazení jednoho vybrané dne je nejvyužívanější možností, kde výsledky (počty Eventů) jsou seskupeny po jednotlivých hodinách.

  Vzhledem k častému využívání a pro okamžitý přehled o aktuálním stavu vytvořených Eventů a Incidentů je tato analýza zobrazena na úvodní stránce, kde jsou však k dispozici pouze grafy, bez detailů po jednotlivých atributech.

- **jedna vybraná hodina**

  Vzhledem k tomu, že záplavy Eventů, tj. abnormality, bývají časově omezeny a trvají většinou max. několik (desítek) minut, je implementována možnost zobrazení pouze jedné vybrané hodiny, kde jsou výsledky (počty Eventů) seskupeny po minutách.

7.9.2 Opakované Eventy a Incidenty

Analýza, která umožňuje vyhledávat opakující se Eventy a zejména Incidenty (Incident tikety), je nejvyužívanější analýzou, jelikož na jejím základě lze upravovat nastavení monitoringu a díky odstranění příčiny opakujících se Incidentů i přímo snižovat náklady.

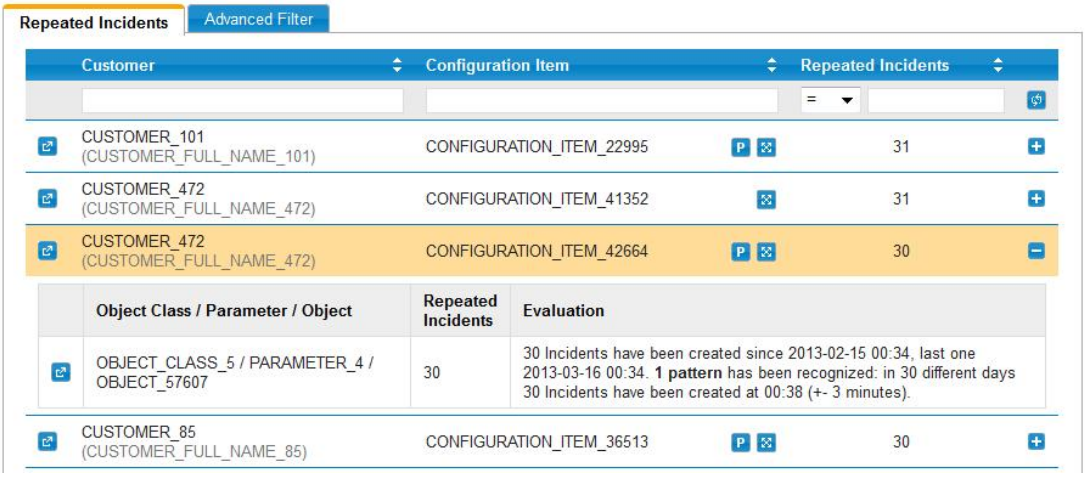
Ve společnosti Tieto je analýza opakujících se Incidentů prováděna na denní bázi určenými specialisty, v případě nalezení opakujících se Incidentů, pro které neexistuje záznam ve znalostní databázi a není otevřen Problem tiket, tito specialisté Problem tiket vytvoří a provedou prvotní analýzu příčiny problému.

Před Event Analytics byly pro vyhledávání opakujících se Incidentů ve společnosti Tieto používány různé nástroje, **po nasazení Event Analytics do produkčního prostředí a zaškolení specialistů byl počet Problem tiketů vytvořených na základě analýzy zvýšen o 100% při současném snížení času vynaloženého na analýzy o 75%.**

Výstupem této analýzy jsou:

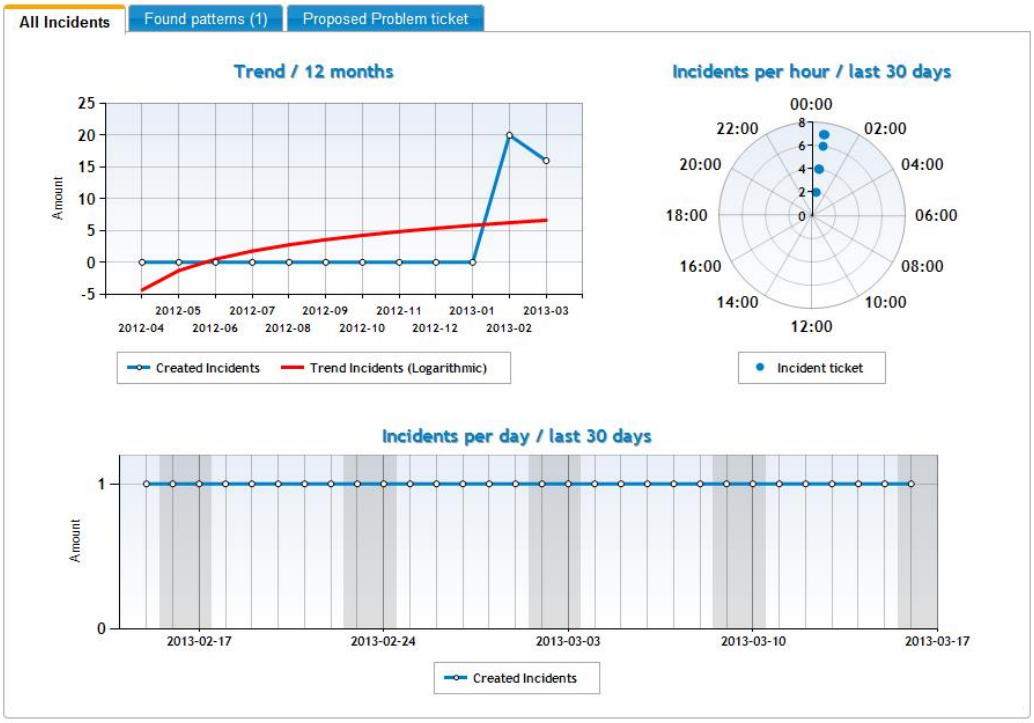
- V tabulkovém přehledu **seznam všech opakujících se Incident tiketů,** tj. Eventů ze kterých byl vytvořen Incident tiket a u kterých jsou shodné atributy Object Class, Parameter a Object, vyhodnocované zvlášť pro každou Konfigurační položku.

- **Nalezené vzory**, tj. Incident tikety opakující se v pravidelných časových intervalech. V tabulkovém přehledu jsou tyto nalezené vzory vyhodnoceny v textovém provedení, v detailním přehledu jsou poté vzory zobrazeny na grafech, kde jeden graf zobrazuje po jednotlivých dnech počty Incident tiketů vytvořených za definovanou dobu a druhý graf zobrazuje čas, tj. hodinu a minutu, ve kterých byly Incident tikety vytvořeny.



Obrázek č. 14 – Tabulkový výpis opakujících se Incident tiketů s textovým vyhodnocením

- U grafického zobrazení je k dispozici **dlouhodobý trend vývoje vybraného Incident tiketu** (po jednotlivých měsících), včetně přehledu za posledních 30 dní (po jednotlivých dnech) a přehled za posledních 30 dní dle času (hodiny a minuty) vytvoření. Dále jsou k dispozici v grafickém zobrazení (za posledních 30 dní, po dnech a času) i jednotlivé nalezené vzory. Vzhledem k tomu, že po zpracování této analýzy uživatelem je nejčastěji vytvářen Problem tiket, je zde automaticky připraven vzor, jak by měl Problem tiket být vyplněn, takže uživatel může zkopírovat předpřipravený text do Problem tiketu.



Obrázek č. 15 – Grafické zobrazení vybraného opakujícího se Incident tiketu

V případě Eventů z databáze Dropped Events je analýza prováděna odlišným způsobem. Jak již bylo zmíněno, tato databáze obsahuje cca 100x více záznamů než databáze History Events, a to jsou data ukládány pouze po omezenou dobu. Díky tomuto množství nebylo možné zpracovávat Eventy stejným způsobem jako v případě databáze History Events.

Druhým specifikem databáze Dropped Events je odlišný charakter Eventů v této databázi. Databáze History Events obsahuje Eventy velkého množství typů, tj. atributy Object Class, Parameter a Object jsou velmi variabilní. Databáze Dropped Events naproti tomu obsahuje poměrně malý počet typů Eventů. Toto je způsobeno tím, že Eventy jsou do databáze Dropped Events ukládány na základě filtrů, kde je přesně definováno, jaké typy Eventů se zde ukládají.

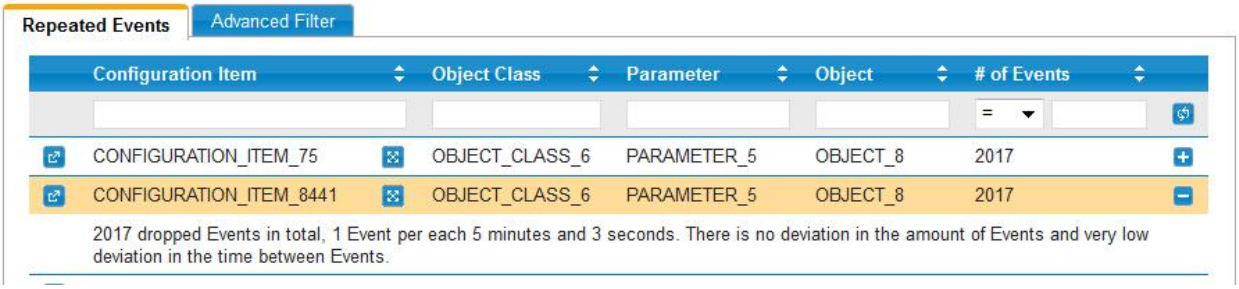
Proto je v databázi Dropped Events daleko větší pravděpodobnost nalezení opakujících se Eventů, a jejich množství je v některých případech i o několik řádů vyšší než v případě databáze Dropped Events. Z tohoto důvodu je implementována jiná metoda pro nalezení vzorů.

Metoda použitá v databázi History Events se snaží nalézt vzory, které jsou podmnožinou nalezených Eventů, kde vzorů může být i více než jeden, přičemž jeden Event může patřit pouze do jediného vzoru.

Naproti tomu metoda použitá v databázi Dropped Events pracuje na všech nalezených Eventech najednou za použití zejména směrodatné odchylky a korelačního koeficientu, nevyhledává podmnožiny.

Tato metoda pro detekci, zda se jedná o opakující se Event, používá následují hodnoty, které jsou počítány vlastní agregační funkcí importovanou do MS SQL Serveru, jak je popsáno v kapitole 7.2:

- korelační koeficient počítaný na základě času vytvoření Eventu a jeho pořadí;
- odchylka časové vzdálenosti mezi jednotlivými Eventy, počítána jako % vůči průměrné časové vzdálenosti Eventů;
- odchylka počtu Eventů za minutu, počítána jako % vůči průměrnému počtu Eventů za minutu.



Obrázek č. 16 – Analýzy opakujících se Eventů v databázi Dropped Events

Jak je vidět na obrázku č. 16 výše, vyhodnocení analýzy je textové, vybraný výsledek analýze lze interpretovat tak, že se jedná Event generovaný každých 5 minut a 3 sekundy, velmi pravidelně (very low deviation in the time) a zároveň množství Eventů za časovou jednotku je pokaždé stejné (no deviation in the amount).

Pro grafické zobrazení je možno použít ikonu , která zobrazí jednotlivé Eventy za posledních 14 dní ve zobrazení popsaném v kapitole 7.9.1.

7.9.3 Dočasné Incidenty

Jako dočasné Incidenty jsou brány Incidenty, kde abnormalita detekovaná monitorovacím softwarem je automaticky opravena předtím, než k opravě dojde manuální akcí. V častých případech představují takovéto dočasné Incidenty zbytečnou manuální práci, tj. zbytečný Incident tiket.

Monitorovací nástroje používané ve společnosti Tieto mají možnost nastavovat zpoždění, tj. posečkat o určený časový interval, zda dojde k automatické opravě abnormality. Teprve po uplynutí této doby, pokud nedošlo k automatické opravě, vytvořit Event, ze kterého je následně vytvořen Incident tiket.

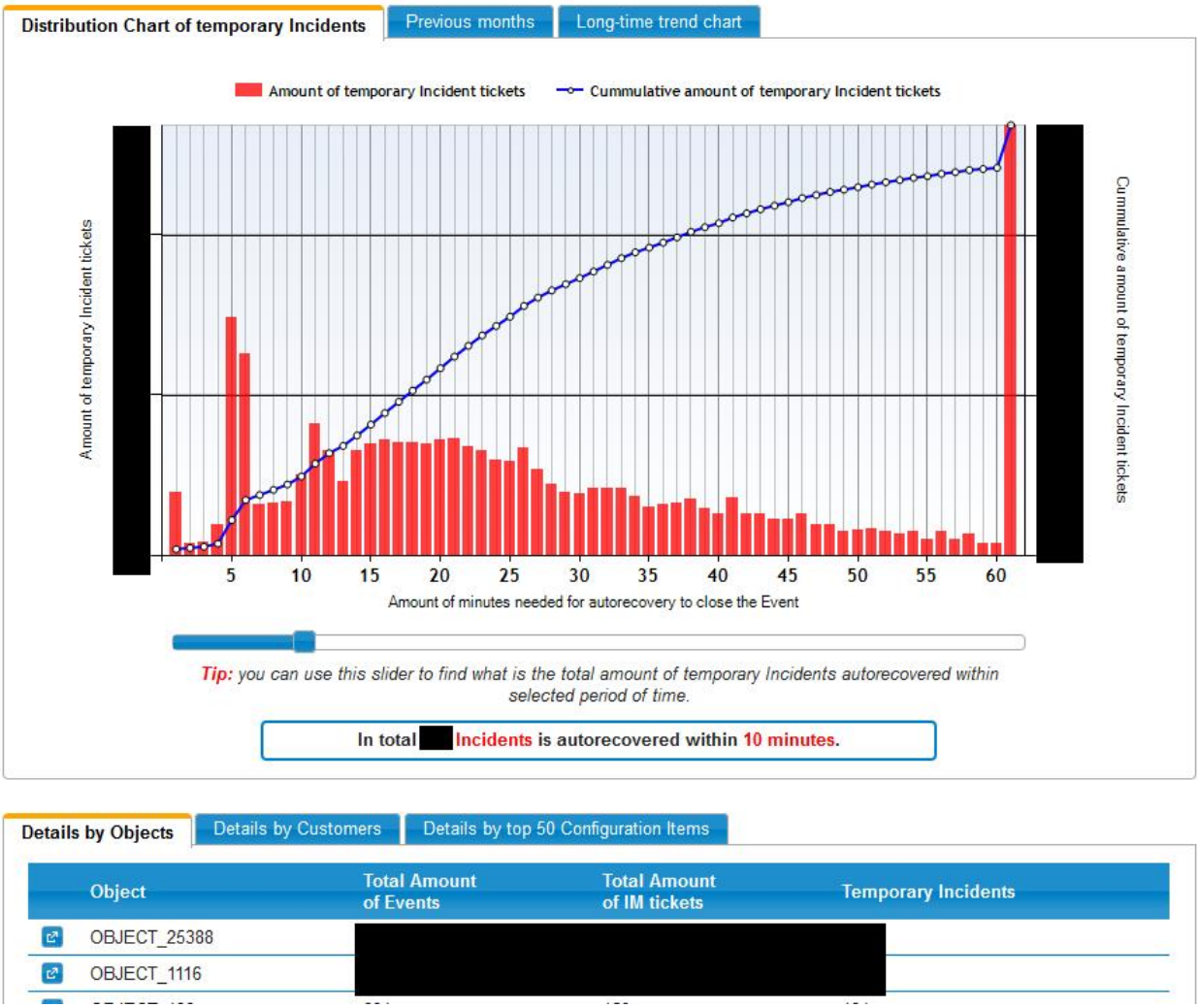
Analýza dočasných Incidentů má za úkol najít právě takového Incidenty, a umožnit na základě výsledků analýzy rozhodnutí, zda a o kolik by bylo vhodné posečkat s vytvořením Eventu. Výsledek poskytnutý Event Analytics je však pouze jeden ze vstupů nutných pro rozhodnutí, je nutno vzít v úvahu další okolnosti, zejména zda je vůbec možné a vhodné posečkat s vytvořením Eventu.

Tato analýza je **z hlediska implementace jedna z náročnějších**, zejména z pohledu času potřebného na její provedení. Během analýzy jsou posuzovány všechny kombinace atributů Object Class, Parameter a Object, které jsou dostupné v minimálním množství definovaném pro tuto analýzu.

Vzhledem k tomu, že nastavení monitoringu se může lišit zákazník od zákazníka, jsou do analýzy přidány ještě atributy Customer a Configuration Item. Přidání těchto atributů sice značně zvýšilo náročnost výpočtů, avšak umožnilo lepší využití výsledků analýzy.

V rámci této analýzy jsou všechny výsledky, včetně hodnot v grafech, předpočítány a uloženy databáze ve formátu XML, takže uživatel má k výsledkům analýzy okamžitý přístup.

Na následujícím obrázku č. 17 jsou zobrazeny výsledky pro vybraný atribut Object Class a Parameter. Pro zobrazení výsledků jsem zvolil upravený graf Pareto, rozdíl je pouze v řažení hodnot, které nejsou od nejvyšší k nejnižší, ale z důvodu přehlednosti jsou ponechány tak, jak za sebou logicky následují, tj. podle počtu minut na ose X, nikoliv podle hodnoty na ose Y.



Obrázek č. 17 – Analýza dočasných Incidentů

Jak je z výsledku analýzy na obrázku č. 17 patrné, velké množství Incidentů je automaticky opraveno již během prvních 5 či 6 minut, což by v tomto případě byla rozumná hranice pro nastavení posečkání na monitorovacím software. Pokud jsou výsledky tohoto typu analýzy rozumně implementovány, je zde jednoznačný přínos ve snížení počtu automaticky generovaných Incident tiketů.

Pro sledování dlouhodobého vývoje počtu dočasných Incidentů, a pro možnost posuzování úspěšnosti přijatých opatření, je možno zobrazit výsledky zpětně za 24 měsíců (hodnotu lze konfigurovat), a to jak ve formě zobrazné na obrázku č. 17, tak i ve formě dlouhodobého trendu počtu Incident tiketů vs. počtu dočasných Incidentů.

Implementace posečkání s vytvořením Eventu přímo v monitorovacím software má ale i svá negativa, a to v možnosti snížení kvality monitoringu. V případě nastavení posečkání na monitorovacím software, za předpokladu delšího časového úseku, by mohla však nastat situace, kdy dochází k opakované abnormalitě, která je však vždy automaticky opravena a z důvodu posečkání není nikdy vytvořen Event a následně Incident tiket.

Z tohoto důvodu je vhodnější posečkání na monitorovacím software nenastavovat, ale implementovat jej přímo do Event Management systému. Implementace Event Managementu ve společnosti Tieto tuto funkcionalitu umožňuje, a proto je možno z důvodu zabezpečení kvality poskytovaných služeb výsledky této analýzy implementovat následujícím způsobem:

- v monitorovacím software nastavit generování Eventu ihned, jakmile je abnormalita detekována;

- v Event Management systému nastavit pozdržení pro takto definované Eventy, kde pokud dojde k automatické opravě abnormality během definované časového intervalu, je Event automaticky uzavřen, v opačném případě je dále zpracován a je vytvořen Incident tiket;

- implementovat počítadlo, které bude počítat počet jednotlivých typů Eventů (zvlášť pro každou Konfigurační položku) a pokud počet Eventů automaticky uzavřených bez vytvoření Incident tiketu překročí definovanou hranici (např. 3x za 24 hodin), vytvořit Incident tiket.

Stav počítadla není potřeba kontrolovat pokaždé, jakmile je některý Event uzavřen, ale je možno jej kontrolovat v pravidelných intervalech. Počítadlo proto může být implementováno dvěma způsoby:

- **v Event Management systému**

  Jak již bylo zmíněno v této diplomové práci, Event Management systém ve společnosti Tieto nemá strukturu dat vhodnou pro analýzy, struktura dat a rozložení indexů je přizpůsobeno rychlému zpracování jednotlivých Eventů.

  Při implementaci této funkce do Event Management systému by mohlo díky zvýšeným potřebám indexace dojít ke zpomalení Event Management systému a tím ke snížení průchodnosti, tj. snížení počtu Eventů zpracovaných za časovou jednotku.

- **v Event Analytics**

  Vzhledem ke skutečnosti, že abnormalita byla automaticky opravena a tím je i poskytována IT služba funkční, není potřeba okamžité reakce. Díky této skutečnosti lze kontrolu počítadla provádět v pravidelných časových intervalech.

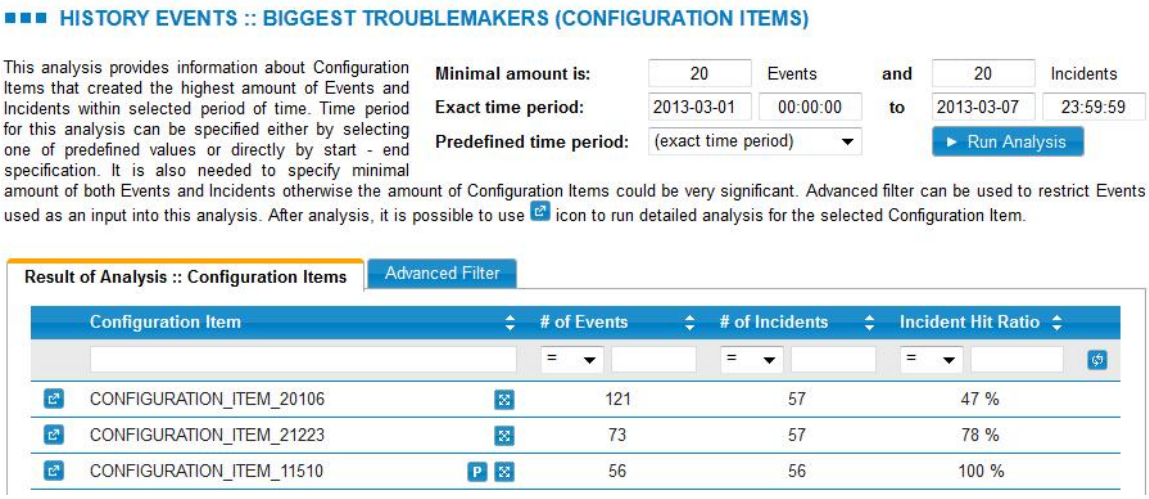
  Event Analytics umožňuje nastavovat automatické reakce, jejich výsledkem je vytvoření definovaného Incident tiketu. Proto lze toto počítadlo implementovat prostřednictvím Event Analytics, kde mohou být i komplexní nastavení zpracována v krátkém čase díky vysokému pokrytí databáze indexy. Funkcionalita automatických reakcí je popsána v kapitole 7.10.

7.9.4 Konfigurační položky s nejvyšším počtem Eventů a Incidentů

Požadavek na tuto analýzy vyplývá z Paretova principu, který lze v tomto případě formulovat tak, že 80% všech Incidentů (Incident tiketů) generuje 20% Konfiguračních položek. Na základě tohoto principu má nejvyšší přínos oprava příčiny těch Incidentů u těch Konfiguračních položek, u kterých je generováno nejvyšší množství Incident tiketů. A právě takovéto Konfigurační položky jsou výsledkem této analýzy.

Konfigurační položky s nejvyšším množství Eventů a Incidentů jsou primárním cílem této analýzy, ale může nastat i situace, kdy je z určité Konfigurační položky generováno velké množství Eventů, avšak žádné Incident tikety.

Může se jednat o Eventy, které jsou odfiltrovány jako nedůležité, případně se může jednat o chyby v Event Management systému apod. Implementována analýza takovéto Eventy umí odhalit díky parametru „Incident Hit Ratio %“, tj. poměr počtu Incident tiketů vůči počtu Eventů, v procentech.



Obrázek č. 18 – Analýza Konfiguračních položek s nejvyšším počtem Eventů a Incidentů

Výstupem této analýzy, u které si uživatel může zvolit vstupní parametry, je seznam Konfiguračních položek s počtem Eventů a Incident tiketů a jejich poměr. Tato analýza nemá vlastní grafické zobrazení detailů, ale ikona u jména Konfigurační položky umožnuje spustit kompletní analýzu Konfigurační položky, která poskytne všechny potřebné informace. Tato analýza je popsána v kapitole 7.9.6.

Kromě Konfiguračních položek je možno tuto analýzu provést i pro zákazníky, kdy výsledkem není seznam Konfiguračních položek, ale seznam zákazníků. Ikona poté analogicky ke Konfiguračním položkám spustí kompletní analázu zákazníka, která je popsána v kapitole 7.9.7.

7.9.5 Analýza záplav

Záplavou se míní krátkodobé zvýšení počtu generovaných Eventů, kdy zvýšení může činit i desítky tisíc procent oproti normálnímu počtu generovaných Eventů. Už ze samotné povahy záplavy, kdy jsou Eventy generovány ze značného množství Konfiguračních položek najednou, vyplývá, že s nejvyšší pravděpodobností mají stejnou příčinu. Nejčastěji se jedná o výpadek kritického síťového zařízení, pád diskového pole apod., tj. výpadky, které mají okamžitý vliv na chod značného množství Konfiguračních položek a které vedou k Major Incidentům.

Analýza záplav má za cíl **nalézt takové Eventy, které by záplavu Eventů indikovaly ještě předtím, než k ní dojde**. Pokud se podaří takovýto Event nalézt, je možno do Event Management systému implementovat pravidla, která by umožnila okamžitou reakci na takovouto situaci, např. vytvořením Incident tiketu s kritickou prioritou, zasláním SMS odpovědným osobám apod.

Event Analytics umožňuje nastavit dva typy detekce záplav:

- **statickou metodou**, kdy se nastaví absolutní počet Eventů za minutu, které již znamenají záplavu;
- **dynamickou metodou**, kde Event Analytics použije horní hranici z „normálního průběhu“, tj. středních 60% hodnot, a nastaví se procento překročení této hranice, které již znamená záplavu.

Dalším nastavovaným parametrem je časový interval počítaný od začátku detekované záplavy, ve kterém se mají vyhledávat jednotlivé Eventy, které potenciálně indikují záplavu. Nejprve je ale nutno pochopit, jak funguje monitorovací software používaný ve společnosti Tieto.

Monitoring není prováděn nepřetržitě, protože by to neúměrně zatěžovalo monitorovaný server či jiné zařízení. Monitoring je prováděn v intervalech, jejichž rozpětí závisí na důležitosti monitorované aplikace apod. Může tedy nastat situace, kdy Event indikující záplavu je generován nikoliv před začátkem záplavy, ale až v jejím průběhu.

Přestože tato situace, kdy indikující Event je generován až v průběhu záplavy, není ideální, může takto indikovaný Event pomoci ne v rychlejší detekci záplavy, ale díky analýze předcházejících situací a připraveným instrukcím umožnit rychlejší nalezení příčiny záplavy a tím i řešení samotné situace.

Z tohoto důvodu Event Analytics umožňuje nastavit časový interval pro vyhledávání Eventů, které potenciálně indikují záplavu, nejenom před začátkem záplavy, ale i na dobu po jejím začátku.

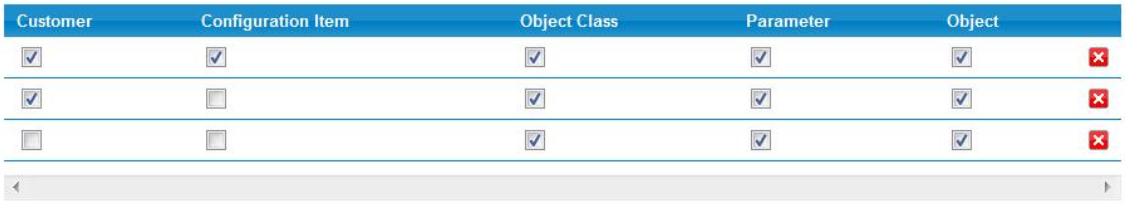
Další situací, se kterou bylo nutno se vypořádat je, že Event indikující záplavu Eventů nemusí pokaždé přijít ze stejné Konfigurační položky nebo zákazníka. Tato situace nenastává často, ale přesto k ní dochází.

Během manuálních analýz záplav Eventů bylo specialisty na UNIX platformu ve společnosti Tieto zjištěno, že sekvence dvou specifických Eventů generovaných krátce po sobě ze serverů používajících operační systém AIX předchází globálnímu výpadku SAN diskového pole. Tyto dva Eventy mohou být generovány jakoukoliv Konfigurační položku, tj. serverem používajícím operační systém AIX.

Při hledání Eventů, které indikují záplavu, se využívá následujících pěti atributů:

- Customer
- Configuration Item
- Object Class
- Parameter
- Object

Aby bylo možné provést i analýzu popsanou na příkladu AIX operačního systému výše, tj. vyhledávat i Eventy z různých Konfiguračních položek či zákazníků, bylo nutno v Event Analytics implementovat hashovací funkci, která na základě nastavených parametrů analýzy (vybraných kombinací uvedených pěti atributů) spočítá pro každý Event hash, který je následně v analýze používán pro zjištění, zda jsou Eventy shodné či ne. Způsob nastavování kombinací atributů je zobrazen na obrázku č. 19 níže.

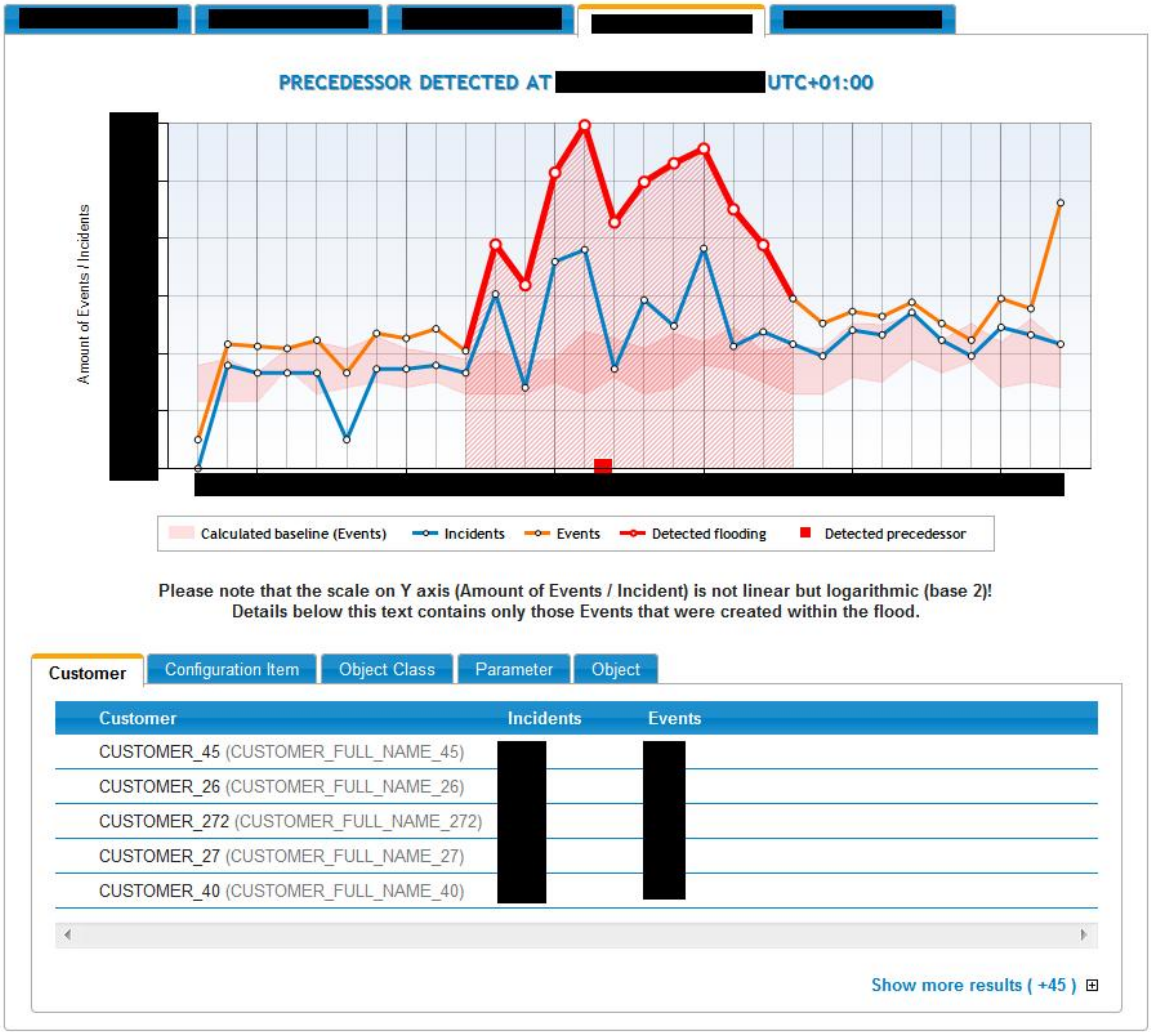


Obrázek č. 19 – Nastavování kombinací atributů pro hashovací funkci

Pro zobrazení pouze relevantních výsledků je v konfiguraci této analýzy možnost nastavit minimální počet, kolikrát musel být Event generován a zároveň minimální spolehlivost, tj. poměr, kolikrát Event potenciálně indikoval záplavu Eventů oproti celkovému počtu, kolikrát byl Event generován.

Výstupem analýzy je na první úrovni tabulka, ve které jsou vypsány jednotlivé Eventy, které byly zjištěny, že mohou indikovat záplavu Eventů, s uvedením jejich spolehlivosti. Po vybrání Eventu jsou poté v grafické podobě zobrazeny detaily o jednotlivých záplavách, jak je vidět na obrázku č. 20.

V grafu je zvýrazněna oblast, která byla Event Analytics detekována jako záplava Eventů, ve spodní části grafu, přímo na ose X, je vyznačena pozice Eventu, který tuto záplavu indikoval. Pod grafem jsou zobrazeny detaily o Eventech, které byly v průběhu záplavy generovány, a ze kterých lze odvodit rozsah záplavy, tj. kteří zákazníci byli ovlivněni a k jakým typům Eventů během záplavy došlo.



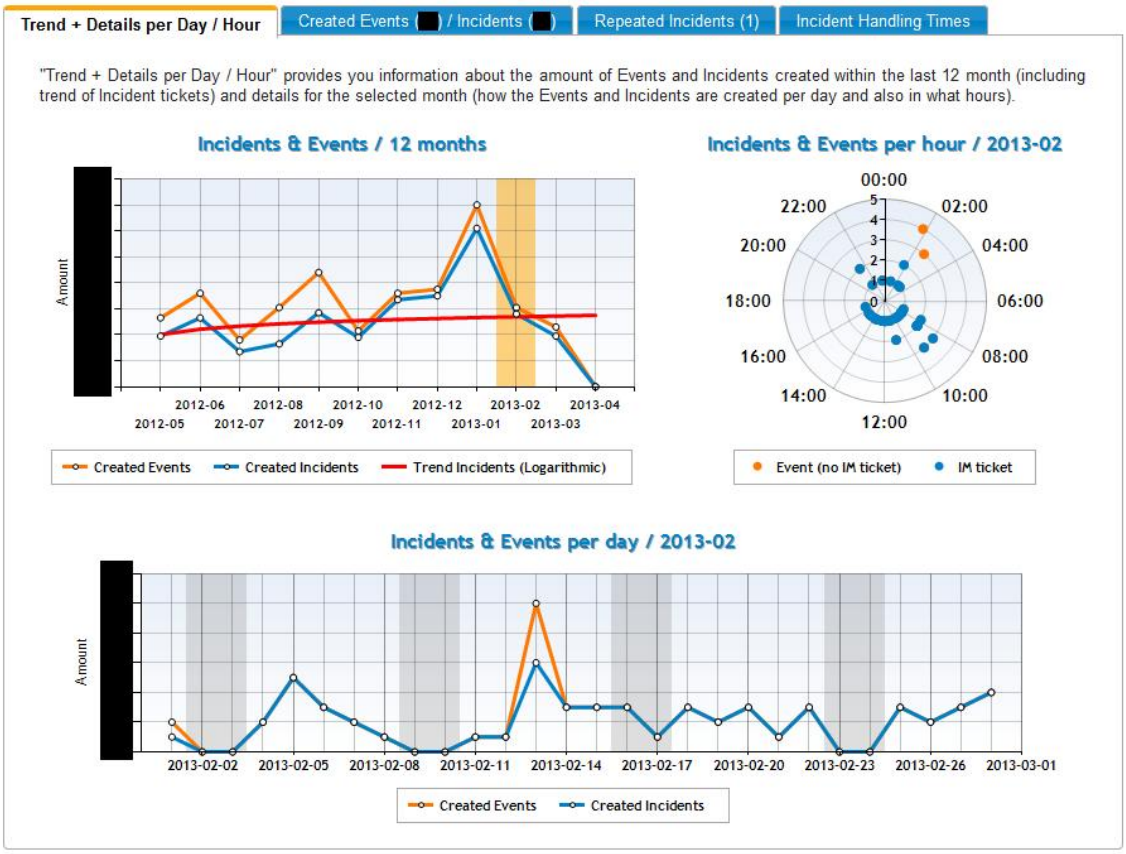
Obrázek č. 20 – Grafické zobrazení výsledku analýzy záplav

Jak z hlediska implementace, tak z hlediska potřebných zdrojů (čas potřebný na analýzu, vytížení CPU, RAM atd.) **se jedná o nejkomplikovanější implementovanou analýzu**. Po spuštění analýzy v produkčním prostředí bylo na jejím základě detekováno několik desítek Eventů, které **se 100% spolehlivostí indikují záplavu Eventů**.

7.9.6 Analýza Konfigurační položky

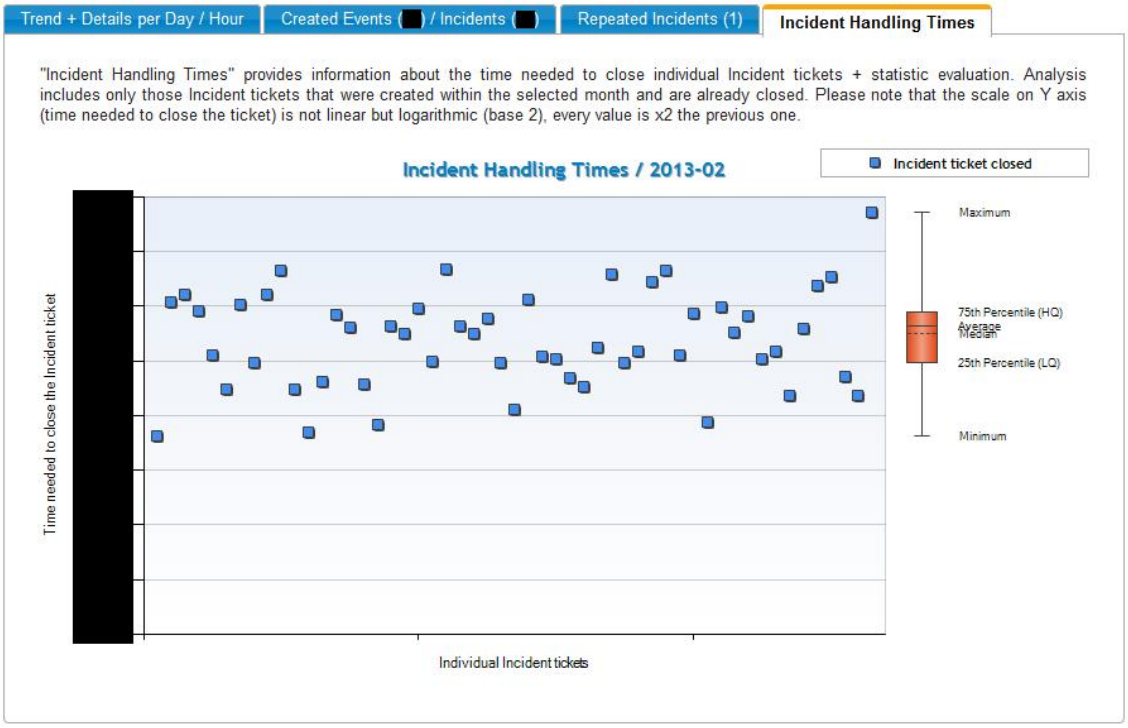
Analýza Konfigurační položky je spolu s analýzou opakovaných Incidentů nejpoužívanější analýzou implementovanou v Event Analytics. V rámci této jediné analýzy jsou zobrazeny nejdůležitější informace potřebné k získání přehledu o Eventech a Incident tiketech generovaných vybranou Konfigurační položkou. Výstupem této analýzy jsou:

- dlouhodobý přehled ohledně počtu generovaných Eventů a Incident tiketů, včetně trendu;
- detailní přehled ohledně počtu generovaných Eventů a Incident tiketů pro vybraný měsíc (po jednotlivých dnech), s vyhodnocením časů jejich generování;
- tabulkový výpis generovaných Eventů po jednotlivých typech, včetně počtu Incident tiketů z nich vytvořených;
- opakující se Incidenty;
- odfiltrované Eventy;
- statistické vyhodnocení časů potřebných na vyřešení Incident tiketů.



Obrázek č. 21 – Analýza Konfigurační položky, dlouhodobý trend a detaily pro vybraný měsíc

Ve výchozím nastavení jsou dlouhodobý trend a detaily pro vybraný měsíc zobrazeny pro všechny Eventy dohromady. V případě potřeby zjištění dlouhodobého vývoje či detailů pro specifický Event lze na záložce „Created Events / Incidents“ viditelné na obrázku č. 21 specifikovat Event, pro který se má dlouhodobý trend a detaily pro vybraný měsíc zobrazit. Tato specifikace Eventu vlivní i výsledky zobrazené na záložce „Incident handling times“, která je zobrazena na obrázku č. 22.



Obrázek č. 22 – Analýza Konfigurační položky, záložka „Incident Handling Times“

Jak jsem již uvedl na začátku této kapitoly, jedná se o jednu z nejpoužívanějších implementovaných analýz. Díky komplexnímu pohledu na aktuální stav a historii generovaných Eventů pro Konfigurační položku je tato analýza velmi často využívána jako doplněk k ostatní implementovaným analýzám, pro lepší interpretaci jejich výsledků.

7.9.7 Analýza zákazníka

Analýza zákazníka je rozšířením analýzy Konfigurační položky, analyzovány jsou Eventy ze všech Konfiguračních položek vybraného zákazníka dohromady. Jsou k dispozici stejná zobrazení jako v případě analýzy Konfigurační položky, pouze s drobnými modifikacemi vzhledem k násobně vyššímu počtu Eventů, což by mohlo vést k nepřehlednosti některých grafů.

Analýza zákazníka má následující odlišnosti oproti analýze Konfigurační položky:

- zobrazení detailů po hodinách, jak je viditelné na obrázku č. 21, graf vpravo nahoře, je vzhledem k množství Eventů nepřehledné, proto je k dispozici tabulkové zobrazení počtu Eventů a Incident tiketů po hodinách;
- jsou zobrazeny všechny Konfigurační položky zákazníka s počtem Eventů a Incident tiketů, včetně jejich poměru (Incident Hit Ratio);
- opakované Incidenty jsou zobrazeny jak po jednotlivých Konfiguračních položkách vybraného zákazníka, tak i z pohledu typu Eventu.

7.10 Automatické reakce

Event Analytics umožňuje nastavení automatických reakcí, jejichý výsledekem je vytvoření specifického Eventu, který je prostřednictvím instalovaného monitorovacího software BMC Patrol zaslán ke zpracování do Event Management systému. Na základě tohoto Eventu je následně provedena jedna či více definovaných akcí, jak je popsáno v kapitole 4.4. V naprosté většině případu se jedná o vytvoření specifického Incident tiketu.

Automatické reakce mohou být nastaveny pro dva základní scénáře:

- **sekvence Eventů**, a to jak v náhodném tak i přesném pořadí;
- **překročení definovaného množství Eventů**.

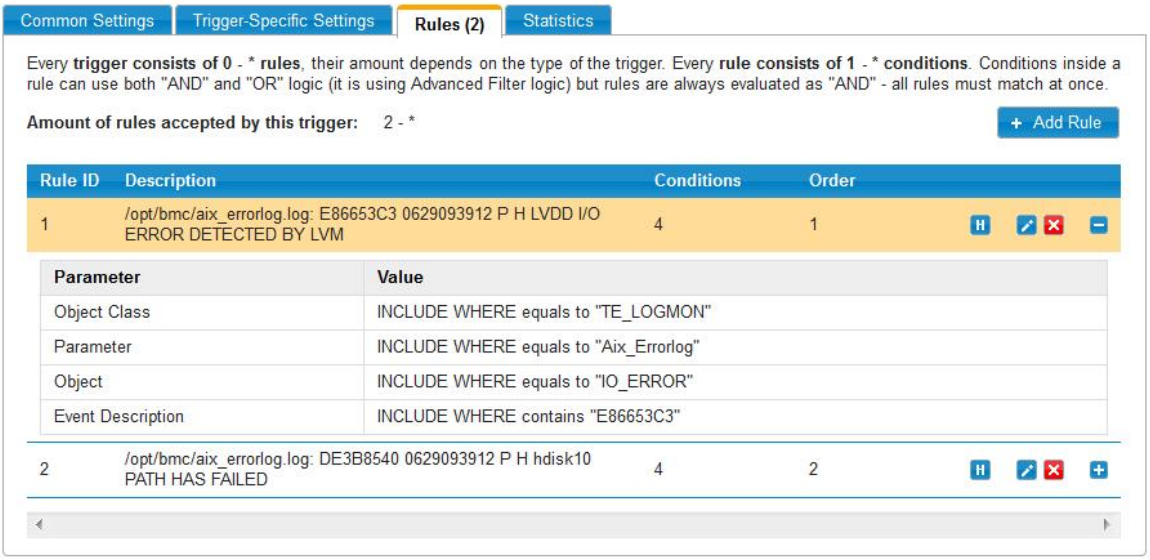
Vyhodnocování jednotlivých nastavených automatických reakcí může být provedeno jedním z následujících tří způsobů:

- **globální**, tj. všechny Eventy jsou posuzovány dohromady;
- **po zákaznících**, tj. každý zákazník je posuzován zvlášť;
- **po Konfiguračních položkách**, tj. každá Konfigurační položka je posuzována zvlášť.

Pro definici pravidel v automatických reakcích je použito Rozšířeného fitru, tj. stejné komponenty, která je v Event Analytics používána pro filtrování výsledků analýz či k omezování vstupních dat.

Pro nastavení automatické reakce u scénáře sekvence Eventů je nutno definovat minimálně 2 pravidla, pro scénář překročení definovaného množství Eventů není nastavení pravidel podmínkou, v tomto případě je brán absolutní počet všech Eventů.

Každé z pravidel se skládá z jedné či více podmínek, které jsou posuzovány společně, a pouze v případě splnění všech podmínek je splněno celé pravidlo. Příklad nastavených pravidel a podmínek je na obrázku č. 22.



Obrázek č. 22 – Nastavování pravidel a podmínek pro automatické reakce

V nastavení automatických reakcí je nutno specifikovat časový interval, tj. v případě scénáře sekvence Eventů rozpětí mezi posledním Eventem prvního pravidla a prvním Eventem posledního pravidla nebo v případě scénáře překročení definovaného možství se jedná o časový interval, ve kterém musí být absolutní množství Eventů překročeno.

Tento časový interval je použit pro nastavení způsobu zpracování automatické reakce, tj. pro způsob, kterým jsou hledány a zpracovány Eventy pro jednotlivá nastavená pravidla. Zpracování probíhá jedním z následujících způsobů:

- **jednotlivě**

  V případě krátkých časových intervalů, zejména pokud je nastavený časový interval kratší než je interval pro synchronizaci, musí být vyhodnocení nastavených pravidel prováděno po jednotlivých Eventech.

- **skupinově, po minutách**

  Pokud je nastavený časový interval max. několik hodin (přesná hodnota závisí na aktuální konfiguraci), je vyhodnocení provedeno skupinově, tj. nejsou vyhodnocovány jednotlivé Eventy a jejich kombinace, ale je použito agregační funkce GROUP BY a Eventy jsou seskupeny po minutách.

Tento způsob zpracování může za určitých okolností vykazovat jiné počty Eventů za určený časový interval než v případě zpracování jednotlivých Eventů, což je způsobeno zaokrouhlováním času vytvoření Eventu pro rychlejší zpracování.

Díky použitému způsobu zaokrouhlování popsanému v kapitole 7.5 nemůže nastat situace, kdy by v případě vyhodnocování po jednotlivých Eventech byl výsledek pozitivní a ve skupinovém zpracování negativní. Může nastat pouze opačná situace, kdy výsledek skupinového zpracování je pozitivní, i když při zpracování metodou jednotlivých Eventů by byl negativní.

Pro lepší pochopení této situace uvedu následující příklad:

Je nastaveno pravidlo, na základě kterého se má vytvořit Incident tiket v případě, že absolutní počet Eventů za 1 hodinu je roven či překročí hodnotu 1000. Skupinovou metodou bylo nalezeno přesně 1000 Eventů, kde první a poslední Event mají následující časy vytvoření:

	Čas vytvoření	*Zakrouhlený čas*
První Event	10:00:20	10:00:00
Poslední Event	11:00:50	11:00:00
Rozdíl	01:00:30	01:00:00

Jak je z tabulky časů vidět, v případě posuzování po jednotlivých Eventech, kdy se počítá s přesným časem vytvoření, by uvedených 1000 Eventů bylo generováno za 1 hodinu a 30 sekund, takže výsledek je negativní. Ale v případě použití skupinové metody je uvedených 1000 Eventů generováno během přesně 1 hodiny, a výsledek je tedy pozitivní.

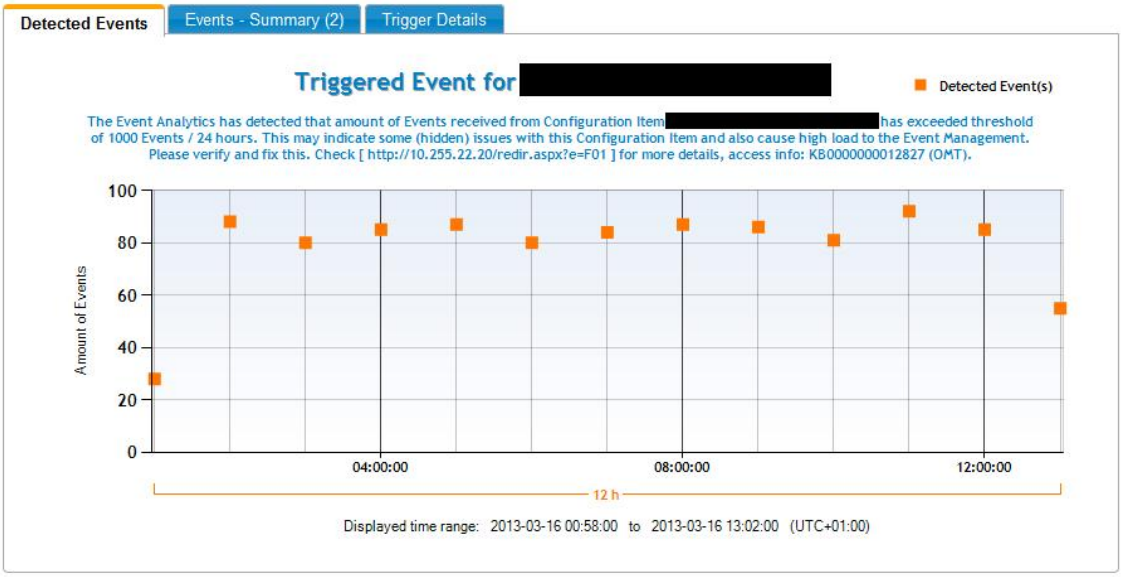
I přes výše uvedenou možnost falešně pozitivních výsledků byla tato metoda implementována, a to z důvodu značně rychlejšího zpracování jednotlivých automatických reakcí.

- **všechny najednou**

  V případě dlouhého časového intervalu, který značně přesahuje dobu mezi synchronizacemi dat, je počítán absolutní počet Eventů mezi časem vytvoření posledního Eventu uloženého v databázi a tímto časem mínus nastavený časový interval. Tato metoda zpracování je ze všech tří metod nejrychlejší.

Event vytvořený na základě pozitivního výsledku vyhodnocení automatické reakce, a následně i vytvořený Incident tiket, obsahuje kromě textu definovaného v konfiguraci automatické reakce i odkaz na detaily, které je možno zobrazit v Event Analytics.

Specialista řešící takto vytvořený Incident tiket má tedy rychlý přístup k informacím o Eventech, které vedly k vytvoření tohoto Incident tiketu. V detailním zobrazení jsou v grafické podobě zaznamenány počty Eventů, které vedly k pozitivnímu výsledku automatické reakce, v textové podobě poté informace, o jaké typy Eventů se jedná.



Obrázek č. 23 – Detail Eventu vytvořeného na základě automatické reakce

Automatické reakce, které byly implementovány v produkčním prostředí ve společnosti Tieto, pomohly zásadně redukovat celkové množství Eventů, které je denně zpracováváno Event Management systémem. A to hlavně díky automatickým reakcím nastaveným na množství Eventů za časovou jednotku, jejichž příklad je vidět na obrázku č. 23 výše.

Díky těmto automatickým reakcím je možno velice rychle reagovat na situace, kdy dochází ke generování velkého množství stejných, opakujících se Eventů. Jelikož dochází v Event Management systému k odfiltrování takovýchto Eventů jako duplicitních, a je vytvořen pouze jediný Incident tiket, nemusí být takovéto chování rychle odhalitelné. Nastavené automatické reakce však toto chování zachytí a umožní tak jeho rychlou opravu.

7.11 Rozšířené informace o Konfigurační položce

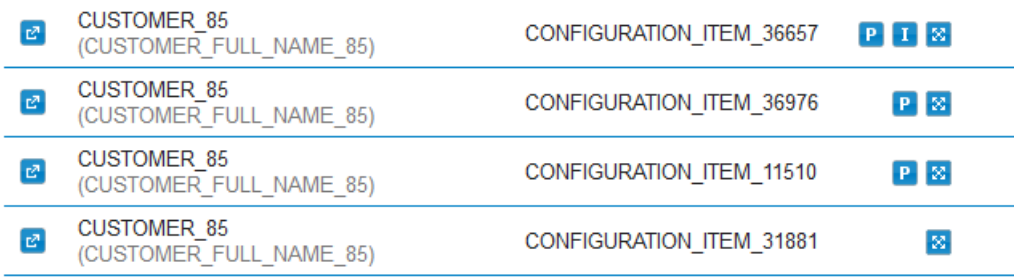
Jak již bylo uvedeno v předcházejících kapitolách, na základě analýzy Eventů provedené v Event Analytics je velmi často vytvořen Problem tiket, na jehož základě je zjišťována příčina problémů, která je následně řešena prostřednictví Change Management procesu, tj. vytvořením Change tiketu.

Tento postup je popsána v kapitole 5.1, kde je zakreslen na obrázku č. 6. První aktivitou, která musí být provedena před vytvořením Problem tiketu, je kontrola, zda již Problem tiket nebyl v minulosti otevřen, a zda je ještě aktivní.

Další informace, které jsou pro specialisty pracující s Event Analytics a Konfiguračními položkami důležité, jsou:

- kterému zákazníkovi Konfigurační položka patří;
- v jaké fázi životního cyklu se Konfigurační položka nachází;
- které skupiny specialistů jsou za ni odpovědné na jednotlivých úrovních.

Pro usnadnění práce s Event Analytics a pro poskytnutí těchto údajů se u každé Konfigurační položky zobrazují jedna až tři ikony.



Obrázek č. 24 – Ikony u jména Konfigurační položky

Pokud pro Konfigurační položku existuje Problem tiket, který je aktivní, tj. ještě není vyřešen, je zobrazena ikona P. Po kliknutí na tuto ikonu jsou tyto Problem tikety zobrazeny s následujícími informacemi:

- číslo Problem tiketu;
- čas vytvoření;
- aktuální stav řešení;
- popis problému;
- dočasné řešení;
- příčina.

Tyto informace jsou pro specialisty dostatečné k tomu, aby mohli rozhodnout, zda vytvořit nový Problem tiket či ne.

Ikona I indikuje, že během poslední několika dní (jedná se konfigurovatelný parametr) byl pro tuto Konfigurační položku vytvořen Event či Eventy na základě nastavených automatických reakcí. Po kliknutí na ikonu jsou tyto Eventy zobrazeny, včetně informací o automatické reakci, na jejímž základě byl Event vytvořen.

Pokud uživatel potřebuje zobrazit informace ohledně vybrané Konfigurační položky, může použít ikonu . Po kliknutí jsou kromě zobrazených informací k dispozici přímé odkazy na další analýzy, které mohou být pro Konfigurační položku přímo spuštěny, jak je vidět na obrázku č. 25.

Obrázek č. 25 – Informace o Konfigurační položce

8 Závěr

Cílem diplomové práce byla analýza, návrh a implementace softwaru pro analýzu automaticky generovaných Eventů ve společnosti Tieto, ve které v současné době pracuji na pozici Senior Process Manager odpovědný za Event Management proces.

Jelikož společnost Tieto, stejně jako ostatní obdobné společnosti, implementuje procesy podle ITIL, byla doporučení obsažená v ITIL V3, knize Service Operation, vzata jako základ toho, které analýzy by měly být implementovány. Jelikož však každá reálná implementace Event Managementu je odlišná, liší se v jednotlivých detailech, byla tato doporučení rozšířena jak o mé vlastní požadavky, které vyplývají z mé náplně práce, tak i o požadavky mnoha týmů ve společnosti Tieto.

Software Event Analytics byl postupně uváděn do provozu od května 2012 a jednotlivé analýzy byly postupně přidávány až do dokončení první verze v dubnu 2013, která je zahrnuta v této diplomové práci. Během této doby jsem obdržel hodně pozitivních ohlasů, včetně velkého množství nápadů na nové funkce, z nichž většina byla v rámci této diplomové práce implementována.

Již během prvních měsíců provozu byl jasně zřetelný přínos Event Analytics pro společnost Tieto, kdy u týmu odpovědného za analýzy Eventů a automaticky vytvářených Incident tiketů došlo ke skokovému zvýšení počtu vytvářených Problem tiketů o více jak 100% při současném snížení potřebného času o 75%.

Na základě implementovaných automatických reakcí bylo možno rychle reagovat na situace, kdy docházelo k zaplavování Event Management systému duplicitními Eventy, a tím umožnit plynulý chod Event Management systému.

Jelikož přínos Event Analytics pro Event Management proces ve společnosti Tieto je jednoznačně pozitivní, budu na vývoji Event Analytics pokračovat implementováním analytických funkcí, které z časových důvodů nebylo možno implementovat v rámci této diplomové práce.

9 Použitá literatura

[1] TIETO. *Tieto Czech* [online]. © 2013 [cit. 2013-03-23]. Dostupné z: http://ww.tieto.cz

[2] OMNICOM S.R.O. *ITSM – Řízení IT služeb* [online]. © 2008-2013 [cit. 2013-03-23]. Dostupné z*:* http://www.itsmportal.cz

[3] *ITIL® v3 : Slovníček termínů, definic a zkratek*. Praha : ItSMF Czech Republic, o.s., 2008. 74 s.

[4] *Service Operation*. United Kingdom : The Stationery Office, 2007. 263 s. ISBN 978-0-11-331046-3.

[5] BERKA, Petr. *Dobývání znalostí z databází.* Vyd. 1. Praha: Academia, 2003, 366 s. ISBN 80-200-1062-9.